Πάτρα, 27/11/2024
Αριθμ. Πρωτ.: 3523

ΠΕΡΙΦΕΡΕΙΑΚΟ ΤΑΜΕΙΟ ΑΝΑΠΤΥΞΗΣ
ΠΕΡΙΦΕΡΕΙΑΣ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
Ν.Π.Ι.Δ
Ν.Ε.Ο. Πατρών-Αθηνών 32 & Αμερικής
Τ.Κ. 26441, Πάτρα
Πληροφορίες: Δ. Μιχαλόπουλος,
Ε. Αθανασοπούλου
Τηλ.: 2613 613635, 2613 613624
Fax: 2610 461126

ΑΝΑΚΟΙΝΩΣΗ υπ' αριθμ. ΣΜΕ 1/2024

για τη σύναψη ΣΥΜΒΑΣΗΣ ΜΙΣΘΩΣΗΣ ΕΡΓΟΥ στο πλαίσιο του ευρωπαϊκού έργου ENDURANCE

Ο Πρόεδρος του Δ.Σ. του Περιφερειακού Ταμείου Ανάπτυξης Περιφέρειας Δυτικής Ελλάδας

Έχοντας υπόψη:

1. Τις διατάξεις του άρθρου 6 του Ν. 2527/1997 (ΦΕΚ 206 Α') περί συμβάσεων μίσθωσης έργου, όπως ισχύουν.

2. Τις διατάξεις του άρθρου 30 του Ν. 4314/2014 (ΦΕΚ 265 Α') περί συμβάσεων Μίσθωσης Έργου σε συγχρηματοδοτούμενες πράξεις, όπως ισχύουν.

3. Τις διατάξεις του Ν. 4765/2021 (ΦΕΚ 6 Α'), όπως ισχύουν.

4. Τις διατάξεις του Π.Δ.. 85/2022 «Καθορισμός προσόντων διορισμού σε φορείς του Δημοσίου (Προσοντολόγιο - Κλαδολόγιο)» (ΦΕΚ 232 Α').

5. Τις διατάξεις των άρθρων 53-56 του Νόμου 2218/1994 (ΦΕΚ 90Α) «Ίδρυση Νομαρχιακής Αυτοδιοίκησης, τροποποίηση διατάξεων για την πρωτοβάθμια αυτοδιοίκηση και την Περιφέρεια και άλλες διατάξεις».

6. Τις διατάξεις των άρθρων 190-193 του Ν.3852/2010 (ΦΕΚ 87Α/07-06-2010) περί «Νέας Αρχιτεκτονικής της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης» και ειδικότερα το άρθρο 193 περί Οργάνωσης – Κανονισμών και Προσωπικού των Περιφερειακών Ταμείων Ανάπτυξης.

7. Την υπ. αριθμ. 4683/1998 (ΦΕΚ 140Β) Απόφαση ΥΠ.ΕΣ.Δ.Δ.Α που αφορά στον Κανονισμό Προσωπικού των Περιφερειακών Ταμείων Ανάπτυξης, όπως τροποποιήθηκε και ισχύει.

8. Την υπ. αριθ. 287493/19 (ΦΕΚ 384 Β'/10-2-2020) Απόφαση του Συντονιστή Αποκεντρωμένης Διοίκησης Πελοποννήσου, Δυτικής Ελλάδας και Ιονίου με θέμα «Τροποποίηση της 93394/14-

5-2019 (Β 2368) απόφασης του Συντονιστή Αποκεντρωμένης Διοίκησης Πελοποννήσου, Δυτικής Ελλάδας και Ιονίου περί Έγκρισης Κανονισμού Προσωπικού του ΠΤΑ/ΠΔΕ», όπως αυτή τροποποιήθηκε με την υπ. αριθ. 207815/21-12-2020 (ΦΕΚ 5608 Β') όμοια απόφαση.

9. Τις διατάξεις του Ν.4727/2020 (ΦΕΚ Α' 184/23.09.2020) «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.

10. Το Ν.4412/2016 (ΦΕΚ 147 Α') «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)».

11. Το Ν.4622/2019 (ΦΕΚ 133 Α') «Επιτελικό Κράτος: οργάνωση, λειτουργία και διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων και της κεντρικής δημόσιας διοίκησης».

12. Τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

13. Το Ν.4624/2019 (ΦΕΚ 137 Α΄) με τίτλο «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις», όπως κάθε φορά ισχύει.

14. Τις διατάξεις του ν. 4914/2022 (ΦΕΚ 61 Α΄) «Διαχείριση, έλεγχος και εφαρμογή αναπτυξιακών παρεμβάσεων για την Προγραμματική Περίοδο 2021-2027, σύσταση Ανώνυμης Εταιρείας "Εθνικό Μητρώο Νεοφυών Επιχειρήσεων Α.Ε." και άλλες διατάξεις».

15. Τις διατάξεις της υπ' αρ. 114947/2022 Υπουργικής Απόφασης (ΦΕΚ 6132 Β') περί Εθνικών κανόνων επιλεξιμότητας δαπανών για τα προγράμματα του ΕΣΠΑ 2021-2027.

16. Τις διατάξεις του Ν.4387/16 (ΦΕΚ 85/Α/12-05-2016) «Ενιαίο Σύστημα Κοινωνικής Ασφάλειας - Μεταρρύθμιση ασφαλιστικού - συνταξιοδοτικού συστήματος - Ρυθμίσεις φορολογίας εισοδήματος και τυχερών παιγνίων και άλλες διατάξεις», όπως ισχύουν.

17. Την 21/2014 Απόφαση του ΔΣ του ΠΤΑ/ΠΔΕ (ΑΔΑ ΒΙΡΝΟΡΕΒ-ΙΜ4) περί προσδιορισμού του ωρομισθίου του έκτακτου προσωπικού που προσλαμβάνεται με ΣΜΕ για την εκτέλεση Ευρωπαϊκών Προγραμμάτων, όπως αυτή τροποποιήθηκε με την υπ. αριθ. 45/2017 Απόφαση του Δ.Σ. του ΠΤΑ-ΠΔΕ (ΑΔΑ 70ΞΚΟΡΕΒ-ΛΨΩ).

18. Το εγκεκριμένο τεχνικό δελτίο του έργου ENDURANCE (κωδικός έργου 101168007 – HORIZON-CL3-2023-INFRA-01).

19. Τον προϋπολογισμό του έτους 2024 του ΠΤΑ/ΠΔΕ (ΑΔΑ 6ΙΛΟΟΡΕΒ-6ΛΘ).

20. Την υπ' αρ. 39/2024 απόφαση του Δ.Σ. του ΠΤΑ/ΠΔΕ (ΑΔΑ 6ΥΥΖΟΡΕΒ-6Σ3).

Ανακοινώνει

Τη σύναψη σύμβασης μίσθωσης έργου με συνολικά ένα (1) άτομο για την κάλυψη αναγκών του Περιφερειακού Ταμείου Ανάπτυξης Περιφέρειας Δυτικής Ελλάδας (ΠΤΑ/ΠΔΕ), που εδρεύει στην Πάτρα, και συγκεκριμένα για την υλοποίηση του ευρωπαϊκού έργου ENDURANCE (Strategies and Tools for Enhanced Disruption Resilience and Cooperation in Europe) που έχει εγκριθεί για χρηματοδότηση στο πλαίσιο του προγράμματος HORIZON EUROPE.

Το έργο ENDURANCE έχει χρονοδιάγραμμα υλοποίησης 36 μηνών, από 1/10/2024 έως 30/9/2027. Στο εταιρικό σχήμα συμμετέχουν δημόσιοι και ιδιωτικοί οργανισμοί από Σλοβενία, Ιταλία, Ρουμανία και Ελλάδα. Ενδεικτικά αναφέρονται από Ελλάδα το ΠΤΑ Αττικής, η ΕΥΔΑΠ και το Ερευνητικό Πανεπιστημιακό Ινστιτούτο Συστημάτων Επικοινωνιών και Υπολογιστών του ΕΜΠ, από Σλοβενία ο Οργανισμός Δικτύων και Υπηρεσιών Επικοινωνίας της Δημοκρατίας της Σλοβενίας, το Κυβερνητικό Γραφείο Ασφάλειας Πληροφοριών της Δημοκρατίας της Σλοβενίας και η Telecom Σλοβενίας, από πλευράς Ιταλίας η αυτόνομη Περιφέρεια Friuli Venezia Giulia και το INSIEL, και από Ρουμανία η Εθνική Διεύθυνση για την Κυβερνοασφάλεια και η εταιρία EVIDEN TECHNOLOGIES η οποία είναι και ο συντονιστής εταίρος του έργου.

Ο σκοπός του έργου είναι να αναλύσει σε βάθος τις αλληλεξαρτήσεις διαφόρων βασικών υπηρεσιών στις συμμετέχουσες περιοχές και τις σχετικές απειλές και κινδύνους, αναπτύσσοντας ολοκληρωμένες μεθοδολογίες, διαλειτουργικά εργαλεία και ρεαλιστικές στρατηγικές για την ενίσχυση της ανθεκτικότητάς τους.

Στο πλαίσιο του έργου προβλέπεται η πιλοτική δοκιμή των προτεινόμενων μεθοδολογιών, σχεδίων και εργαλείων σε επιλεγμένους τομείς για να διασφαλιστεί η αποτελεσματικότητά τους στον πραγματικό κόσμο. Στην Ελλάδα η πιλοτική εφαρμογή θα αφορά στον τομέα της διαχείρισης υδάτινων πόρων και υγρών αποβλήτων.

Στο έργο προβλέπεται επίσης και η ανάπτυξη ολοκληρωμένου εκπαιδευτικού υλικού και κατευθυντήριων γραμμών για την ενδυνάμωση των ενδιαφερόμενων μερών με γνώσεις και

δεξιότητες για την αποτελεσματικότερη προετοιμασία τους στην αντιμετώπιση διαταραχών και κινδύνων.

Η υλοποίηση του έργου διακρίνεται σε συνολικά δώδεκα (12) πακέτα εργασίας με τους εξής τίτλους:

WP1 - COOPERATION: Strategic Collaboration & Cooperation (Phase 1), με παραδοτέα: D1.1 – European Disruption Resilience Snapshot

WP2 - COOPERATION: Strategic Collaboration & Cooperation (Phase 2), με παραδοτέα: D2.1 – Draft - European Disruption Resilience Strategy, D2.2 – European Disruption Resilience Strategy

WP3 - *ROADMAP: Technical & Strategic Oversight (Phase 1),* με παραδοτέα: D3.1 – Data Management Plan, D3.2 – Roadmap Towards TRL5

WP4 - *ROADMAP: Technical & Strategic Oversight (Phase 2),* με παραδοτέα: D4.1 – Roadmap Towards TRL6, D4.2 – Roadmap Towards TRL7

WP5 - ENABLERS: Disruption Resilience Enablers (Phase 1), με παραδοτέα: D5.1 – Enablers Prototypes

WP6 - ENABLERS: Disruption Resilience Enablers (Phase 2), με παραδοτέα: D6.1 – ENDURANCE Enablers

WP7 - SERVICES: Disruption Resilience Services (Phase 1), με παραδοτέα: D7.1 – Service Prototypes

WP8 - SERVICES: Disruption Resilience Services (Phase 2), με παραδοτέα: D8.1 – ENDURANCE Services, D8.2 – ENDURANCE Services (Sensitive)

WP9 - PILOTS: Large-Scale & Cross-X Exercises (Phase 1 - reaching TRL5), με παραδοτέα: D9.1 – Test Designs and Plans, D9.2 – First Pilot Report, D9.3 – First Pilot Report (Sensitive)

WP10 - PILOTS: Large-Scale & Cross-X Exercises (Phase 2 - reaching TRL7), με παραδοτέα: D10.1 – Second Pilot Report, D10.2 – Second Pilot Report (Sensitive), D10.3 – Final Pilot Report, D10.4 – Final Pilot Report (Sensitive)

WP11 - IMPACT: Impact Generation, με παραδοτέα: D11.1 – Brand, Website, and Social Media Channels, D11.2 – Impact Generation Strategy, D11.3 – Impact Assessment Methodology, D11.4 – Impact Assessment, Business Plan, and Sustainability Roadmap

WP12 - MANAGEMENT: Project Coordination, με παραδοτέα: D12.1 – Project Handbook, D12.2 – Compliance Analysis and Guidelines, D12.3 – Compliance Assessment and Policy Recommendations

WP13 - Ethics requirements, με παραδοτέα: D13.1 – OEI - Requirement No. 1, D13.2 – OEI - Requirement No. 2, D13.3 – OEI - Requirement No. 3, D13.4 – OEI - Requirement No. 4

Το ΠΤΑ-ΠΔΕ έχει ενεργό συμμετοχή και συνεισφορά στα πακέτα εργασίας WP1, WP2, WP3, WP4, WP9, WP10, WP11 & WP12, ενώ λαμβάνει γνώση και παρακολουθεί και την υλοποίηση των υπολοίπων πακέτων εργασίας, καθότι είναι άρρηκτα συνδεδεμένα με την εξέλιξη και υλοποίηση του έργου (WP5, WP6, WP7, WP8), είτε αφορούν σε οριζόντιες δεσμεύσεις για όλους τους εταίρους (WP13).

Αναλυτικότερα, το σχέδιο υλοποίησης του έργου, η περιγραφή των πακέτων εργασίας και των δράσεων ανά εταίρο περιγράφονται αναλυτικά στο συνημμένο τεχνικό δελτίο του έργου (DoA).

Στο πλαίσιο του έργου αυτού θα απασχοληθεί ανά τόπο εκτέλεσης, ειδικότητα και διάρκεια σύμβασης ο εξής αριθμός ατόμων (βλ. ΠΙΝΑΚΑ Α), με τα αντίστοιχα απαιτούμενα (τυπικά και τυχόν πρόσθετα) προσόντα (βλ. ΠΙΝΑΚΑ Β):

Α) ένα άτομο κατηγορίας ΠΕ που θα αναλάβει την καθημερινή παρακολούθηση της πορείας εκτέλεσης του έργου και την υποστήριξη της ομάδας έργου του ΠΤΑ-ΠΔΕ στην υλοποίηση όλων των παραδοτέων του έργου στα οποία συμμετέχει ενεργά το ΠΤΑ-ΠΔΕ, μέχρι την ολοκλήρωση του έργου (ήτοι έως 30/9/2027). Ειδικότερα, το άτομο αυτό θα έχει συμβολή στην υλοποίηση των παραδοτέων D1.1, D.2,1, D.2.2, D3.1, D3.2, D.4.1, D.4.2, D.9.1, D.9.2, D.9.3, D.10.1, D.10.2, D.10.3, D.10.4, D.11.1, D.11.2, D.11.3, D.11.4, D.12.1, D.12.2, και D.12.3. Η ανώτατη προβλεπόμενη αμοιβή για όλη τη διάρκεια του έργου ανέρχεται στο ποσό των 54.000€ συμπεριλαμβανομένου του ΦΠΑ και των νόμιμων κρατήσεων και εισφορών, ωστόσο η συνολική αμοιβή θα προσδιορισθεί κατά την υπογραφή της σύμβασης με βάση το ωρομίσθιο του απασχολούμενου σύμφωνα με τις αποφάσεις του Δ.Σ. του ΠΤΑ-ΠΔΕ και το συνολικό αριθμό ωρών απασχόλησης που αντιστοιχούν στο παραγόμενο έργο, ο οποίος δεν δύναται να υπερβαίνει τις 1720 ώρες σε ετήσια βάση, κι όχι πλέον της αναφερόμενης ανώτατης αμοιβής.

Στα ανωτέρω ποσά συμπεριλαμβάνονται οι εισφορές του εργαζομένου καθώς και οι εργοδοτικές εισφορές του άρθρου 38 του Ν. 4387/2016, τις οποίες θα καταβάλει ο εργοδότης, σε περίπτωση που ο απασχολούμενος «Ανάδοχος» υπάγεται στη ρύθμιση του ν. 4387/2016, άρθρο 39, παρ. 9.

Τα έξοδα μετακίνησης και διαμονής του απασχολούμενου που αφορούν στο έργο δεν καλύπτονται από την ανωτέρω αμοιβή και θα καταβάλλονται επιπροσθέτως κατόπιν έκδοσης εντολών μετακίνησης του ΠΤΑ/ΠΔΕ, σύμφωνα με την ισχύουσα νομοθεσία περί μετακινούμενων του δημοσίου.

Η αμοιβή καταβάλλεται τμηματικά ανάλογα με την πρόοδο των εργασιών. Προς τούτο ο απασχολούμενος θα συμπληρώνει και θα υπογράφει μηνιαία περιγραφή των εργασιών του (έκθεση πεπραγμένων) ανά παραδοτέο. Σε αυτή θα συνυπογράφουν ο Προϊστάμενος Τμήματος Ποιότητας και Ηλεκτρονικής Διακυβέρνησης, ο Προϊστάμενος Μονάδας Α’ του ΠΤΑ/ΠΔΕ και ο Διευθυντής του φορέα υλοποίησης, οι οποίοι βεβαιώνουν την προσήκουσα εκτέλεση του έργου κατά το αντίστοιχο τμήμα του.

Η καταβολή της αμοιβής θα πραγματοποιείται στην έδρα του ΠΤΑ/ΠΔΕ σύμφωνα με την ισχύουσα Νομοθεσία. Η αμοιβή θα καταβάλλεται μετά την έκδοση και την υποβολή των σχετικών παραστατικών και δικαιολογητικών πληρωμής από τον απασχολούμενο.

Το ΠΤΑ/ΠΔΕ διατηρεί το δικαίωμα να μην εγκρίνει το επί μέρους έργο που η εκτέλεσή του θεωρείται μη αποδεκτή και στη διακριτική του ευχέρεια είναι να ζητήσει την επανάληψη ή αποκατάστασή του.

Ο τόπος παροχής των υπηρεσιών είναι η έδρα του ΠΤΑ/ΠΔΕ ή όπου απαιτηθεί για τις ανάγκες του έργου.

Σε περίπτωση που παραταθεί ο χρόνος υλοποίησης του έργου είναι δυνατή η παράταση της σύμβασης μίσθωσης έργου έως του 50% της αρχικής διάρκειας αυτής, και η μεταβολή (αύξηση) του οικονομικού της αντικειμένου εφόσον υφίσταται αύξηση του φυσικού αντικειμένου, και έως του 50% του αρχικού οικονομικού της αντικειμένου.

Σε κάθε περίπτωση οι συμβατικές υποχρεώσεις του υποψηφίου ολοκληρώνονται με την οριστική υποβολή όλων των προβλεπόμενων παραδοτέων του ΠΤΑ/ΠΔΕ προς τον συντονιστή εταίρο του έργου και την έγκριση αυτών από την αρμόδια υπηρεσία του προγράμματος.

ΠΙΝΑΚΑΣ Α: ΕΠΙΛΟΓΕΣ ΑΠΑΣΧΟΛΗΣΗΣ (ανά κωδικό απασχόλησης)				
Κωδικός απασχόλησης	**Τόπος εκτέλεσης**	**Ειδικότητα**	**Διάρκεια σύμβασης**	**Αριθμός ατόμων**
101	Πάτρα (έδρα του ΠΤΑ)	ΠΕ Διοικητικού – Οικονομικού	μέχρι την ολοκλήρωση του έργου	1

ΠΙΝΑΚΑΣ Β: ΑΠΑΙΤΟΥΜΕΝΑ ΠΡΟΣΟΝΤΑ (ανά κωδικό απασχόλησης)	
Κωδικός απασχόλησης	**Τίτλος σπουδών και λοιπά απαιτούμενα (τυπικά & τυχόν πρόσθετα) προσόντα**
101	**<u>ΚΥΡΙΑ ΠΡΟΣΟΝΤΑ</u>** α) Πτυχίο ή δίπλωμα Πτυχίο ή δίπλωμα οποιοσδήποτε Τμήματος Α.Ε.Ι. της ημεδαπής ή ακαδημαϊκά ισοδύναμος ή ισότιμος τίτλος σχολών της αλλοδαπής β) Κάτοχος μεταπτυχιακού τίτλου σπουδών σε θέματα συναφή με ανάλυση περιβαλλοντικών δεδομένων

ΠΙΝΑΚΑΣ Β: ΑΠΑΙΤΟΥΜΕΝΑ ΠΡΟΣΟΝΤΑ (ανά κωδικό απασχόλησης)	
Κωδικός απασχόλησης	**Τίτλος σπουδών και λοιπά απαιτούμενα (τυπικά & τυχόν πρόσθετα) προσόντα**
	γ) Γνώσεις σε θέματα διαχείρισης/αξιολόγησης κινδύνων από φυσικές ή ανθρωπογενείς καταστροφές ή/και σε θέματα ανάπτυξης σχεδίων προστασίας και ασφάλειας υποδομών ή/και πληροφοριακών συστημάτων δ) Άριστη γνώση της αγγλικής γλώσσας. ε) Γνώση χειρισμού Η/Υ στα αντικείμενα (i) επεξεργασίας κειμένων, (ii) υπολογιστικών φύλλων και (iii) υπηρεσιών διαδικτύου **ΠΡΟΣΟΝΤΑ Α' ΕΠΙΚΟΥΡΙΑΣ:** (Εφόσον δεν καταστεί δυνατή η σύναψη σύμβασης μίσθωσης έργου με άτομο με τα ανωτέρω προσόντα) Τα ανωτέρω κύρια προσόντα με αριθμό α, β, ε και πολύ καλή γνώση αγγλικής.

ΑΠΟΔΕΙΚΤΙΚΑ ΠΡΟΣΟΝΤΩΝ ΕΞΕΙΔΙΚΕΥΜΕΝΗΣ ΓΝΩΣΗΣ ή ΕΜΠΕΙΡΙΑΣ

Το προσόν της εξειδικευμένης γνώσης που ζητείται κατά ειδικότητα στον Πίνακα Β αποδεικνύεται ως ακολούθως:

ΚΩΔΙΚΟΣ ΑΠΑΣΧΟΛΗΣΗΣ	ΤΡΟΠΟΣ ΑΠΟΔΕΙΞΗΣ
101	Πιστοποιητικό επιμόρφωσης δημόσιου ή αναγνωρισμένου ιδιωτικού φορέα σε θέματα διαχείρισης/αξιολόγησης κινδύνων από φυσικές ή ανθρωπογενείς καταστροφές ή/και σε θέματα ανάπτυξης σχεδίων προστασίας και ασφάλειας υποδομών ή/και πληροφοριακών συστημάτων.

ΒΑΘΜΟΛΟΓΗΣΗ ΚΡΙΤΗΡΙΩΝ

Η σειρά κατάταξης μεταξύ των υποψηφίων καθορίζεται με βάση τα ακόλουθα κριτήρια:

ΠΙΝΑΚΑΣ ΒΑΘΜΟΛΟΓΗΣΗΣ ΚΡΙΤΗΡΙΩΝ

1. ΒΑΘΜΟΣ ΔΟΜΗΜΕΝΗΣ ΣΥΝΕΝΤΕΥΞΗΣ (έως 500 μονάδες)

1η θεματική ενότητα	1 – 250
2η θεματική ενότητα	1 - 250

2. ΒΑΘΜΟΣ ΒΑΣΙΚΟΥ ΤΙΤΛΟΥ (για ΠΕ οι μονάδες του βασικού τίτλου με 2 δεκαδικά ψηφία πολλαπλασιάζονται με το 40)

Βαθμός	5	…	5,5	…	6	…	6,5	…	7	…	7,5	…	8	…	8,5	…	9	…	9,5	…	10
μονάδες	200	…	220	…	240	…	260	…	280	…	300	…	320	…	340	…	360	…	380	…	400

3. ΕΜΠΕΙΡΙΑ (7 μονάδες ανά μήνα εμπειρίας και έως 36 μήνες)

μήνες εμπειρίας	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…	35	36 και άνω
μονάδες	7	14	21	28	35	42	49	56	63	70	77	84	91	98	…	245	252

ΕΜΠΕΙΡΙΑ

ΒΑΘΜΟΛΟΓΟΥΜΕΝΗ ΕΜΠΕΙΡΙΑ ΥΠΟΨΗΦΙΩΝ ΚΑΤΗΓΟΡΙΩΝ ΠΕ

Ως βαθμολογούμενη εμπειρία νοείται η απασχόληση με σχέση εργασίας ή σύμβαση έργου στο δημόσιο ή ιδιωτικό τομέα σε **καθήκοντα σχετικά με την διαχείριση/αξιολόγηση κινδύνων και ανάπτυξη σχεδίων προστασίας και ασφάλειας υποδομών ή/και πληροφοριακών συστημάτων**.	
ΚΩΔΙΚΟΣ ΑΠΑΣΧΟΛΗΣΗΣ	**ΕΜΠΕΙΡΙΑ ΚΑΙ ΤΡΟΠΟΣ ΑΠΟΔΕΙΞΗΣ**
101	Η εμπειρία λαμβάνεται υπόψη **μετά τη λήψη του βασικού τίτλου σπουδών** με τον οποίο οι υποψήφιοι μετέχουν στη διαδικασία επιλογής. Για την απόδειξη της εμπειρίας αυτής βλ. δικαιολογητικά **περίπτωση Β ή Ειδικές περιπτώσεις απόδειξης εμπειρίας** του Παραρτήματος ανακοινώσεων Συμβάσεων Μίσθωσης Έργου (ΣΜΕ) - ΚΕΦΑΛΑΙΟ ΙΙ., στοιχείο 7. Πιστοποιητικά απόδειξης εμπειρίας.

Οι τρόποι υπολογισμού της εμπειρίας περιγράφονται αναλυτικά στο «Παράρτημα ανακοινώσεων Συμβάσεων Μίσθωσης Έργου (ΣΜΕ)», με σήμανση έκδοσης «ΣΜΕ.1.2024» (βλ. ΚΕΦΑΛΑΙΟ Ι., ενότητα Ε., υποενότητα «ΤΡΟΠΟΙ ΥΠΟΛΟΓΙΣΜΟΥ ΕΜΠΕΙΡΙΑΣ»).

ΑΠΑΡΑΙΤΗΤΑ ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ

Οι υποψήφιοι για την απόδειξη των ΑΠΑΙΤΟΥΜΕΝΩΝ ΠΡΟΣΟΝΤΩΝ (βλ. ΠΙΝΑΚΑ Β), των λοιπών ιδιοτήτων τους και της εμπειρίας τους οφείλουν να προσκομίσουν όλα τα απαιτούμενα από την παρούσα ανακοίνωση και το «Παράρτημα ανακοινώσεων Συμβάσεων Μίσθωσης Έργου (ΣΜΕ)», με σήμανση έκδοσης «ΣΜΕ.1.2024» δικαιολογητικά, σύμφωνα με τα οριζόμενα στην ενότητα «ΠΡΟΣΚΟΜΙΣΗ ΤΙΤΛΩΝ, ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΒΕΒΑΙΩΣΕΩΝ» του Κεφαλαίου ΙΙ του ανωτέρω Παραρτήματος, με την επιπλέον υποχρέωση υποβολής των δικαιολογητικών απόδειξης εξειδικευμένης εμπειρίας του ανωτέρω πίνακα «ΑΠΟΔΕΙΚΤΙΚΑ ΠΡΟΣΟΝΤΩΝ ΕΞΕΙΔΙΚΕΥΜΕΝΗΣ ΓΝΩΣΗΣ ή ΕΜΠΕΙΡΙΑΣ».

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ: Δημοσίευση της ανακοίνωσης

Περίληψη της παρούσας ανακοίνωσης να δημοσιευθεί στο κατάστημα της Περιφέρειας Δυτικής Ελλάδας και σε δύο (2) τοπικές εφημερίδες ημερήσιας ή εβδομαδιαίας κυκλοφορίας.

Ανάρτηση ολόκληρης της ανακοίνωσης [**μαζί** με το «Παράρτημα ανακοινώσεων Συμβάσεων Μίσθωσης Έργου (ΣΜΕ)» με σήμανση έκδοσης «ΣΜΕ.1.2024», **και** τα Ειδικά Παραρτήματα: Α1 με τίτλο «Απόδειξη Γνώσης Πληροφορικής ή Χειρισμού Η/Υ», Α2 με τίτλο «Απόδειξη Γλωσσομάθειας» και Α3 «Description of the Action (DoA)»] να γίνει στο κατάστημα της υπηρεσίας μας και στην ιστοσελίδα του φορέα μας. Θα συνταχθεί και **σχετικό πρακτικό ανάρτησης στο φορέα**.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ: Υποβολή αιτήσεων συμμετοχής

Οι ενδιαφερόμενοι καλούνται να συμπληρώσουν την αίτηση με κωδικό **ΣΜΕ.1.2024** και να την υποβάλουν αποκλειστικά ηλεκτρονικά σε μορφή pdf μέσω email στη διεύθυνση ptapde@ptapde.gr και θέμα «Υποβολή αίτησης για την ΣΜΕ …….. Ανακοίνωση του Π.Τ.Α./Π.Δ.Ε.

Κάθε υποψήφιος δικαιούται να υποβάλει **μία μόνο αίτηση, με ποινή αποκλεισμού από τη διαδικασία επιλογής σε περίπτωση υποβολής άνω της μίας αιτήσεων**. Η αίτηση συμμετοχής που θα υποβληθεί ηλεκτρονικά πρέπει απαραιτήτως να εμφανίζεται υπογεγραμμένη, με φυσική ή ψηφιακή υπογραφή. Ανυπόγραφες αιτήσεις δεν γίνονται δεκτές.

Επισημαίνεται: ότι σύμφωνα με το νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 γνωστό ως GDPR, που ετέθη σε εφαρμογή τον Μάιο 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ. Για το λόγο αυτό, η συμμετοχή των υποψηφίων στη διαδικασία πρόσληψης με την οικειοθελή υποβολή αίτησης με τα συνημμένα σε αυτή δικαιολογητικά προς τον Φορέα, συνεπάγεται τη συναίνεση του υποψηφίου για τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τους αφορούν, καθώς και για την ασφαλή διατήρησή τους σε αρχείο (φυσικό ή ψηφιακό) για συγκεκριμένο σκοπό και για όσο χρόνο απαιτείται, προκειμένου να ολοκληρωθούν οι νόμιμες διαδικασίες πρόσληψης. Οι φορείς οφείλουν να προστατεύουν τα προσωπικά στοιχεία των υποψηφίων από τυχόν υποκλοπή προκειμένου να επιτυγχάνεται η ασφαλής επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οι υποψήφιοι διατηρούν το δικαίωμα ανάκλησης της συναίνεσής τους ανά πάσα στιγμή και κατόπιν υποβολής σχετικής αίτησης προς το Φορέα.

Η προθεσμία υποβολής των αιτήσεων είναι δώδεκα (12) ημέρες (υπολογιζόμενες ημερολογιακά) και αρχίζει από την επόμενη ημέρα της τελευταίας ανάρτησής της ανάρτησής της στην ιστοσελίδα του φορέα μας. Η ανωτέρω προθεσμία λήγει με την παρέλευση ολόκληρης της τελευταίας ημέρας και εάν αυτή είναι, κατά νόμο, εξαιρετέα (δημόσια αργία) ή μη εργάσιμη, τότε η λήξη της προθεσμίας μετατίθεται την επόμενη εργάσιμη ημέρα.

Οι υποψήφιοι **μπορούν να αναζητήσουν τα έντυπα** των αιτήσεων: **α)** στην υπηρεσία μας στην διεύθυνση·Ν.Ε.Ο. Πατρών-Αθηνών 32 & Αμερικής (1ος όροφος) κατόπιν ραντεβού και **β)** στο δικτυακό τόπο της υπηρεσίας μας (www.ptapde.gr).

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ: Κατάταξη υποψηφίων

Αφού η υπηρεσία μας επεξεργαστεί τις αιτήσεις των υποψηφίων, επιλέγει καταρχάς τους υποψήφιους οι οποίοι διαθέτουν τα κύρια προσόντα της ειδικότητας, και εφόσον δεν υφίστανται, τους έχοντες τα επικουρικά. Στη συνέχεια τους καλεί για τη δομημένη συνέντευξη του Κεφαλαίου ΙΙΙ του παραρτήματος εντός δέκα (10) ημερών από την καταληκτική ημερομηνία υποβολής των αιτήσεων. Η ακριβής ημερομηνία και ο τρόπος εκτέλεσης των συνεντεύξεων θα ανακοινωθεί στην ιστοσελίδα του φορέα (www.ptapde.gr). Κατόπιν της διεξαγωγής των συνεντεύξεων η αρμόδια

επιτροπή που θα συσταθεί για την αξιολόγηση των αιτήσεων κατατάσσει βάσει των κριτηρίων αξιολόγησης όπως αυτά αναλυτικά αναφέρονται στην παρούσα ανακοίνωση. Η **κατάταξη** των υποψηφίων, βάσει της οποίας θα γίνει η **τελική επιλογή** για τη σύναψη της σύμβασης μίσθωσης έργου, πραγματοποιείται ως εξής:

1. **Προηγούνται** στην κατάταξη οι υποψήφιοι που διαθέτουν τα **κύρια προσόντα** της ειδικότητας και ακολουθούν οι έχοντες τα επικουρικά.

2. Η κατάταξη μεταξύ των υποψηφίων που έχουν τα ίδια προσόντα *(κύρια ή επικουρικά)* γίνεται κατά φθίνουσα σειρά με βάση τη **συνολική βαθμολογία** που συγκεντρώνουν από τα βαθμολογούμενα κριτήρια κατάταξης.

3. Στην περίπτωση **ισοβαθμίας** υποψηφίων στη συνολική βαθμολογία προηγείται αυτός που έχει τις περισσότερες μονάδες στο πρώτο βαθμολογούμενο κριτήριο και, αν αυτές συμπίπτουν, αυτός που έχει τις περισσότερες μονάδες στο δεύτερο κριτήριο και ούτω καθεξής. Αν εξαντληθούν όλα τα κριτήρια, η σειρά μεταξύ των υποψηφίων καθορίζεται με δημόσια κλήρωση.

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ: Ανάρτηση πινάκων και υποβολή ενστάσεων

Μετά την κατάρτιση των πινάκων, η υπηρεσία μας **θα αναρτήσει, το αργότερο μέσα σε είκοσι (20) ημέρες από τη λήξη της προθεσμίας υποβολής των αιτήσεων συμμετοχής, τους πίνακες κατάταξης των υποψηφίων** στο κατάστημα των γραφείων μας και στην ιστοσελίδα της υπηρεσίας (www.ptapde.gr), ενώ θα συνταχθεί **και σχετικό πρακτικό ανάρτησης** το οποίο θα υπογραφεί από δύο (2) υπαλλήλους της υπηρεσίας.

Κατά των πινάκων αυτών επιτρέπεται στους ενδιαφερόμενους η άσκηση **ένστασης** μέσα σε αποκλειστική **προθεσμία δέκα (10) ημερών** (υπολογιζόμενες ημερολογιακά) η οποία αρχίζει από την επόμενη ημέρα της ανάρτησής τους. Η ένσταση κατατίθεται αποκλειστικά ηλεκτρονικά στη διεύθυνση ptapde@ptapde.gr και εξετάζεται από το αρμόδιο όργανο.

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ: Απασχόληση

Η υπηρεσία δύναται να προβεί στη σύναψη σύμβασης μίσθωσης έργου με τους επιλεγέντες υποψηφίους **αμέσως μετά** την κατάρτιση των πινάκων κατάταξης. Τυχόν **αναμόρφωση** των πινάκων κατόπιν ένστασης, συνεπάγεται ανακατάταξη των υποψηφίων, εκτελείται **υποχρεωτικά** από το φορέα, ενώ λύεται η σύμβαση μίσθωσης έργου με τους υποψηφίους οι οποίοι δεν δικαιούνται απασχόλησης βάσει της νέας κατάταξης. Οι υποψήφιοι αυτοί λαμβάνουν τις αποδοχές που προβλέπονται για την απασχόλησή τους έως την ημέρα της λύσης της σύμβασης, χωρίς οποιαδήποτε αποζημίωση από την αιτία αυτή.

Απασχολούμενοι που αποχωρούν πριν από τη λήξη της σύμβασής τους, **αντικαθίστανται** με άλλους από τους εγγεγραμμένους και διαθέσιμους στον πίνακα της οικείας ειδικότητας, κατά τη σειρά εγγραφής τους σε αυτόν.

Σε κάθε περίπτωση, οι υποψήφιοι που επιλέγονται είτε κατόπιν αναμόρφωσης των πινάκων είτε λόγω αντικατάστασης αποχωρούντων υποψηφίων, απασχολούνται για το **υπολειπόμενο**, κατά περίπτωση, χρονικό διάστημα και μέχρι συμπληρώσεως της **εγκεκριμένης διάρκειας** της σύμβασης μίσθωσης έργου.

ΑΝΑΠΟΣΠΑΣΤΟ ΤΜΗΜΑ της παρούσας ανακοίνωσης αποτελεί και το *«Παράρτημα ανακοινώσεων Συμβάσεων Μίσθωσης Έργου (ΣΜΕ)»* με σήμανση έκδοσης «ΣΜΕ.1.2024», το

οποίο περιλαμβάνει: i) οδηγίες για τη συμπλήρωση της αίτησης – υπεύθυνης δήλωσης με κωδικό ΣΜΕ.1.2024, σε συνδυασμό με επισημάνσεις σχετικά με τα προσόντα και τα βαθμολογούμενα κριτήρια κατάταξης των υποψηφίων σύμφωνα με τις ισχύουσες κανονιστικές ρυθμίσεις, ii) τα δικαιολογητικά που απαιτούνται για την έγκυρη συμμετοχή τους στη διαδικασία επιλογής και iii) στοιχεία για τη δομημένη συνέντευξη.

Ο Πρόεδρος του ΠΤΑ-ΠΔΕ

Νεκτάριος Φαρμάκης
Περιφερειάρχης Δυτ. Ελλάδας

3/1/2024

ΕΙΔΙΚΟ ΠΑΡΑΡΤΗΜΑ (Α1)
ΑΠΟΔΕΙΞΗΣ ΓΝΩΣΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΄Η ΧΕΙΡΙΣΜΟΥ Η/Υ

- Για όλους τους κλάδους και ειδικότητες των κατηγοριών ΠΕ και ΤΕ και για τους κλάδους και ειδικότητες ΔΕ Διοικητικού–Λογιστικού, ΔΕ Δημοτικής Αστυνομίας, ΔΕ Μεταφραστών – Διερμηνέων, ΔΕ Προσωπικού Ελιγμών, ΔΕ Σταθμαρχών σύμφωνα με το π.δ. 85/2022 (Α΄232) απαιτείται, ως πρόσθετο προσόν διορισμού ή πρόσληψης, η γνώση πληροφορικής ή χειρισμού Η/Υ στα αντικείμενα:

  (α) επεξεργασίας κειμένων,

  (β) υπολογιστικών φύλλων,

  (γ) υπηρεσιών διαδικτύου.

- Για λοιπούς κλάδους και ειδικότητες ΔΕ, μπορεί, με την προκήρυξη πλήρωσης θέσεων, να ορίζεται ως πρόσθετο προσόν διορισμού, η γνώση πληροφορικής ή χειρισμού Η/Υ μετά από αίτημα του φορέα και σύμφωνη γνώμη του ΑΣΕΠ.

Σε περίπτωση που απαιτείται πέραν των ανωτέρω και γνώση συγκεκριμένου προγράμματος ή αντικειμένου πληροφορικής, σχετικού με την κατά περίπτωση ειδικότητα, αυτή καθορίζεται κάθε φορά με την προκήρυξη και αποδεικνύεται με τους τρόπους που ορίζονται σε αυτήν.

Η γνώση πληροφορικής ή χειρισμού Η/Υ και στα ως άνω τρία αντικείμενα διαπιστώνεται ως εξής:

1. Με πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ.
2. Με τίτλους σπουδών, τριτοβάθμιας, μεταδευτεροβάθμιας ή δευτεροβάθμιας εκπαίδευσης, ειδικότητας Πληροφορικής ή γνώσης χειρισμού Η/Υ όπως αυτοί προσδιορίζονται για τους κλάδους ΠΕ Πληροφορικής, ΤΕ Πληροφορικής και ΔΕ Πληροφορικής στους Πίνακες 1, 2 και 3 αντίστοιχα του Παραρτήματος Α΄ του Π.Δ. 85/2022 (Α΄232).
3. Με τίτλους σπουδών, προπτυχιακούς ή/και μεταπτυχιακούς ή/και διδακτορικούς, Πανεπιστημιακής ή/και Τεχνολογικής εκπαίδευσης από την αναλυτική βαθμολογία των οποίων προκύπτει ότι οι υποψήφιοι έχουν παρακολουθήσει τέσσερα τουλάχιστον μαθήματα, υποχρεωτικά ή κατ' επιλογή, Πληροφορικής ή γνώσης χειρισμού Η/Υ.
4. Με Κρατικό Πιστοποιητικό Πληροφορικής (άρθρο 28 ν. 4653/2020).
5. Με πιστοποιητικό αποφοίτησης από την Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ).

Ειδικότερα:

(1) Με πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ που εκδίδονται από φορείς της ημεδαπής οι οποίοι πιστοποιούνται με αποφάσεις του Δ.Σ. του Εθνικού Οργανισμού Πιστοποίησης Προσόντων και Επαγγελματικού Προσανατολισμού (ΕΟΠΠΕΠ), ή ΕΟΠΠ ή τον πρώην Οργανισμό Επαγγελματικής Εκπαίδευσης και Κατάρτισης (ΟΕΕΚ) ή έχουν εκδοθεί από τον ίδιο τον ΟΕΕΚ.

Οι πιστοποιημένοι φορείς από τον ΟΕΕΚ ή τον ΕΟΠΠ ή τον ΕΟΠΠΕΠ, με σχετικές πράξεις, με την αναγραφόμενη για κάθε φορέα ημερομηνία πιστοποίησης, με την επιφύλαξη των αρ. 28 και 40 της με αριθμό 121929/Η/31.07.2014 Κ.Υ.Α (ΦΕΚ 2123/Β'/01.08.2014) και της ΚΥΑ 33198/Κ6/22.03.2023 (ΦΕΚ 1961/Β'/27.03.2023) και τα πιστοποιητικά που εκδίδουν είναι:

α) ACTA Α.Ε. (ΑΡΙΣΤΟΤΕΛΕΙΕΣ ΚΑΤΑΡΤΙΣΕΙΣ ΑΞΙΟΛΟΓΗΣΕΙΣ ΠΙΣΤΟΠΟΙΗΣΕΙΣ Α.Ε.) (17.5.2006)

Πιστοποιητικά:

Certified Computer User (CCU)

Certification Proficiency in IT Skills, CPIT

Microsoft Office Specialist Syllabus 1.0

Microsoft Office Specialist Expert Syllabus 1.0
IC3-Internet and Computing Core Certification Syllabus 1.0
ICBU-Informatics Certified Basic User Syllabus 1.0

β) ACTA-INFOTEST ΠΙΣΤΟΠΟΙΗΣΕΙΣ Ε.Ε. (ΔΠ 54083/16.7.2015 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
Internet and Computing Core Certification (IC3)
Microsoft Office Specialist
Infotest Certified Basic User
Microsoft Certified Application Specialist

γ) DIPLOMA (ΦΟΡΕΑΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ) (30.9.2009)
Πιστοποιητικά:
Basic Office
Business Office

δ) ECDL Ελλάς Α.Ε. (1.2.2006 έως 30.11.2012 βάσει της αριθ. Β/22578/30.11.2012 απόφασης του ΕΟΠΠΕΠ) ή PeopleCert Ελλάς ΑΕ (30.11.2012 με την αριθ. Β/22579/30.11.2012 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
ECDL Core Certificate
ECDL Start Certificate
ECDL Progress Certificate
ECDL Profile Certificate
ECDL Profile Certificate (Office Essentials/Βασικές Δεξιότητες Υπολογιστή)
People Cert Computer Skills Level 1

ε) Ελληνικό Ινστιτούτο Πιστοποιήσεων ΙΚΕ «ΕΛ.ΙΝ.Π.» (ΔΠ/38566/3.9.2018 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
Πληροφορικής/Certified Computer User
CROSS CCU (Certified Computer User) BASIC 1
CROSS CCU (Certified Computer User) BASIC 2

στ) ESOL EXAMS Α.Ε. «ESOL EXAMS» (ΔΠ/60239/05.12.2019 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
STANDARD COMPUTER SKILLS
STANDARD COMPUTER SKILLS FAST
EXCELLENT COMPUTER SKILLS

ζ) «EUROPEAN QUALIFICATIONS CERTIFICATIONS – EQcert – Μ. ΠΙΤΣΙΛΚΑΣ–Κ. ΠΡΙΤΣΑΣ ΙΚΕ Φορέας Πιστοποίησης Ανθρώπινου Δυναμικού» (ΔΠ/2997/17.02.2020 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
EQcert BASIC
EQcert BASIC - LV1
EQcert BASIC - LV2

η) EXAMS CERT ΙΚΕ «EXAMS CERT» (ΔΠ/56579/26.10.2018 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:

EXAMS CERT BASIC
EXAMS CERT BASIC MS
EXAMS CERT PROGRESSIVE EXTRA

θ) GLOBAL CERT (ΠΙΣΤΟΠΟΙΗΣΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ) (10.4.2014)
Πιστοποιητικά:
Global Intermediate
Global Intermediate A
Global Intermediate B
Global Intermediate C
Global Basic Office
Global Advanced Plus
Global Intermediate Express
Global Office Expert

ι) ICT Hellas A.E. (22.2.2006) ή ICT Europe (18.7.2007 αλλαγή ονομασίας της ICT Hellas A.E.)
Πιστοποιητικά:
ICT Intermediate A
ICT Intermediate B
ICT Intermediate C

ια) Infotest (ΑΡΙΣΤΟΤΕΛΕΙΕΣ ΚΑΤΑΡΤΙΣΕΙΣ ΑΞΙΟΛΟΓΗΣΕΙΣ ΠΙΣΤΟΠΟΙΗΣΕΙΣ Α.Ε & ΣΙΑ Ε.Ε.) (22.2.2006)
Πιστοποιητικά:
Internet and Computing Core Certification (IC3)
Microsoft Office Specialist (MOS)
Microsoft Office Specialist Expert (MOS Expert)
Infotest Certified Basic User (ICBU)
Infotest Microsoft Certified Application Specialist

ιβ) «INNOV-INK ΦΟΡΕΑΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΟΣΟΝΤΩΝ ΙΚΕ» με διακριτικό τίτλο PROGRAMS QUALIFICATION READ-PQR (ΔΠ/12126/12.04.2021 απόφαση του ΕΟΠΠΕΠ) ή «INNOV-INK ΦΟΡΕΑΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΙΚΕ» με διακριτικό τίτλο Programs Qualification Read-PQR (27020/17.11.2023 απόφαση του ΕΟΠΠΕΠ)
Πιστοποιητικά:
ELIC Professional Certificate
ELIC Professional Certificate Plus
ELIC Professional Certificate 360

ιγ) I SKILLS A.E. (I SKILLS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΔΕΞΙΟΤΗΤΩΝ) (14.9.2007)
Πιστοποιητικά:
Basic I.T. Standard
Basic I.T. Thematic
Basic I.T. Core
Advanced I.T. Core syllabus version:1 (ΔΠ/27661/22.07.2021 απόφαση του ΕΟΠΠΕΠ)
Advanced I.T. Standard syllabus version:1 (ΔΠ/27661/22.07.2021 απόφαση του ΕΟΠΠΕΠ)
Advanced I.T. Thematic syllabus version:1 (ΔΠ/27661/22.07.2021 απόφαση του ΕΟΠΠΕΠ)

ιδ) KEY-CERT (ΣΥΓΧΡΟΝΕΣ ΕΥΡΩΠΑΙΚΕΣ ΠΙΣΤΟΠΟΙΗΣΕΙΣ Ε.Π.Ε.) (5.4.2006)

Πιστοποιητικά:

Key Cert IT Basic

Key Cert IT Initial

KeyCERT IT Basic Plus

ιε) PROCERT Ιδιωτική Κεφαλαιουχική Εταιρεία «PROCERT» (ΔΠ/20516/4.5.2018 απόφαση του ΕΟΠΠΕΠ)

Πιστοποιητικά:

PRO-Cert IT User

ιστ) ΤΕΛΕΦΩΣ ΤΡΕΙΝΙΝ - TELEFOS TRAINING ΕΠΕ (18-12-2007) ή ΤΕΛΕΦΩΣ ΣΕΡΤ - TELEFOS CERT ΕΠΕ (Με την αριθ.Γ/12485/21.5.2009 πράξη μετονομασίας της ΤΕΛΕΦΩΣ ΤΡΕΙΝΙΝ - TELEFOS TRAINING ΕΠΕ) ή ΙΝΦΟΣΕΡΤ-INFOCERT ΕΠΕ (ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ ΕΤΑΙΡΕΙΑ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΕΥΘΥΝΗΣ) (Με την αριθ. Β/18216/24.9.2012 απόφαση του ΕΟΠΠΕΠ περί μετονομασίας της ΤΕΛΕΦΩΣ ΣΕΡΤ - TELEFOS CERT ΕΠΕ)

Πιστοποιητικά:

Basic Skills ή Infocert Basic Skills (25.6.2008 αλλαγή ονομασίας τίτλου)

Basic ή Infocert Basic (25.6.2008 αλλαγή ονομασίας τίτλου)

Integration Skills ή Infocert Integration Skills (25.6.2008 αλλαγή ονομασίας τίτλου)

Infocert Unities

ιζ) «UCERT» ΜΟΝΟΠΡΟΣΩΠΗ ΙΔΙΩΤΙΚΗ ΚΕΦΑΛΑΙΟΥΧΙΚΗ ΕΤΑΙΡΕΙΑ (ΔΠ/30357/03.08.2020 απόφαση του ΕΟΠΠΕΠ)

Πιστοποιητικά:

STANDARD OFFICE USER

STANDARD OFFICE USER (UPPER LEVEL)

STANDARD OFFICE USER -BLENDED-1

STANDARD OFFICE USER -BLENDED-2

ιη) UNICERT (UNIVERSAL CERTIFICATION SOLUTIONS ΦΟΡΕΑΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ) (21.01.2015)

Πιστοποιητικά:

Unicert Primary

Unicert Primary Διαθεματικό

Unicert Advanced Plus

PRIMARY Διαθεματικό (Διαθεματικό-2)

ιθ) Vellum Global Educational Services S.A. (ΒΕΛΛΟΥΜ ΔΙΕΘΝΕΙΣ ΥΠΗΡΕΣΙΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ Α.Ε.) (22.2.2006), ΒΕΛΛΟΥΜ ΔΙΕΘΝΕΙΣ ΥΠΗΡΕΣΙΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ και Vellum Global Educational Services (ΔΠ 35945/28.7.2017 απόφαση του ΕΟΠΠΕΠ), ΒΕΛΛΟΥΜ ΥΠΗΡΕΣΙΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ Ε.Ε. (ΔΠ 4768/6.3.2023 απόφαση του ΕΟΠΠΠΕΠ)

Πιστοποιητικά:

Cambridge International Diploma in IT Skills

Cambridge International Diploma in IT Skills Proficiency

Vellum Diploma in IT Skills

Vellum Diploma in IT Skills Proficiency

Vellum Diploma in IT Skills Essential Standard Level

κ) «PROFESSIONAL AWARDING SERVICES SOLUTIONS ΜΟΝΟΠΡΟΣΩΠΗ ΙΔΙΩΤΙΚΗ ΚΕΦΑΛΑΙΟΥΧΙΚΗ ΕΤΑΙΡΕΙΑ» με διακριτικό τίτλο «PASS MON IKE (P.A.S.S.) » (ΔΠ/16690/25-11-2022 απόφαση του ΕΟΠΠΕΠ)

Πιστοποιητικά:

PASS-PORT

PASS-PORT FAST-B

PASS-PORT FAST-X

κα) «TÜV-AUSTRIA ΕΛΛΑΣ ΜΟΝΟΠΡΟΣΩΠΗ ΕΤΑΙΡΕΙΑ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΕΥΘΥΝΗΣ» με διακριτικό τίτλο «TÜV AUSTRIA-HELLAS LTD» (ΔΠ/6314/24-03-2023 απόφαση του ΕΟΠΠΕΠ)

Πιστοποιητικά:

TÜV AUSTRIA Certification for basic Computer Skills

ΓΙΝΟΝΤΑΙ ΕΠΙΣΗΣ ΔΕΚΤΑ:

I. Πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ τα οποία χορηγήθηκαν από τους παραπάνω φορείς (δ, ι, ια και ιθ) μέχρι και την ημερομηνία πιστοποίησής τους από τον ΟΕΕΚ με την εξής ονομασία:

α) ECDL από την εταιρεία ECDL-GREEK COMPUTER SOCIETY-Ε.Π.Υ.

β) Cambridge International Examinations από UNIVERSITY OF CAMBRIDGE (εταιρεία Vellum Global Educational Services).

γ) IC3 ή MOS από CERTIPORT (Microsoft), εταιρεία Infotest (πρώην TECHNOPLUS) και

δ) BTEC in ICT ή Online Award in ICT από LONDON LEARNING (εταιρεία ICT Hellas A.E.).

II. Πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ που έχουν εκδοθεί από τον ΟΕΕΚ, κατόπιν επιτυχούς συμμετοχής του υποψηφίου σε εξετάσεις πιστοποίησης Γνώσεων Χειρισμού Η/Υ φυσικών προσώπων που διοργάνωσε ο Οργανισμός.

Σημείωση: Η ισχύς των πιστοποιητικών γνώσης χειρισμού Η/Υ που εκδόθηκαν από τον ΟΕΕΚ, από φορείς πιστοποιημένους από τον καταργηθέντα ΟΕΕΚ μέχρι και την ημερομηνία πιστοποίησής τους και από φορείς πιστοποιημένους από τον ΟΕΕΚ, τον ΕΟΠΠ και τον ΕΟΠΠΕΠ μετά την ημερομηνία πιστοποίησής τους **<u>είναι αόριστης διάρκειας</u>** [παρ. 6 του άρ. 12 του Ν. 4283/2014 (ΦΕΚ 189 Α΄/10-9-2014) όπου αναφέρεται ότι προστίθεται παρ. 5 στο άρ. 38 του Ν.4186/2013].

III. Πιστοποιητικά ή τίτλοι γνώσης πληροφορικής ή χειρισμού Η/Υ που χορηγούνται από φορείς της αλλοδαπής που έχουν αναγνωριστεί με απόφαση του Δ.Σ. του ΕΟΠΕΠΠ. Οι τίτλοι αυτοί γίνονται αποδεκτοί υπό την προϋπόθεση ότι συνοδεύονται από σχετική απόφαση του Δ.Σ. του ΕΟΠΠΕΠ περί της αντιστοίχισης τους με πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ της ημεδαπής.

Από τα ανωτέρω πιστοποιητικά πρέπει να αποδεικνύεται η γνώση <u>και</u> των τριών ενοτήτων: α) επεξεργασίας κειμένων, β) υπολογιστικών φύλλων και γ) υπηρεσιών διαδικτύου (τα πιστοποιητικά μπορούν να περιέχουν οποιονδήποτε συνδυασμό των ενοτήτων «Επεξεργασία Κειμένου», «Υπολογιστικά Φύλλα», «Υπηρεσίες Διαδικτύου»).

Σε περίπτωση που ο υποψήφιος έχει ολοκληρώσει με επιτυχία τις εξετάσεις στις οριζόμενες από την προκήρυξη ενότητες αλλά το σχετικό πιστοποιητικό **δεν έχει ακόμη εκδοθεί**, μπορεί να γίνει αποδεκτή σχετική περί τούτου **βεβαίωση** του κατά τα ανωτέρω πιστοποιημένου φορέα έκδοσης αυτού. Αν ο υποψήφιος επιλεγεί στην ειδικότητα που επιδιώκει, πρέπει να προσκομίσει το πιστοποιητικό στο φορέα πρόσληψης ή ανάθεσης του έργου.

Λοιπά παραστατικά (βεβαιώσεις εξεταστικών κέντρων, κάρτες δεξιοτήτων κ.λπ.) <u>δεν γίνονται δεκτά</u>.

(2) Με τίτλους σπουδών, τριτοβάθμιας, μεταδευτεροβάθμιας ή δευτεροβάθμιας εκπαίδευσης, ειδικότητας Πληροφορικής ή γνώσης χειρισμού Η/Υ, όπως αυτοί προσδιορίζονται για τους κλάδους ΠΕ Πληροφορικής, ΤΕ Πληροφορικής και ΔΕ Πληροφορικής στους Πίνακες 1, 2 και 3 αντίστοιχα του Παραρτήματος Α΄ του ΠΔ 85/2022 (Α΄232) και αναφέρονται κατωτέρω ή μεταπτυχιακούς ή διδακτορικούς τίτλους στην Πληροφορική.

(3) Με τίτλους σπουδών, προπτυχιακούς Πανεπιστημιακής ή/και Τεχνολογικής εκπαίδευσης ή/και μεταπτυχιακούς ή/και διδακτορικούς, από την αναλυτική βαθμολογία των οποίων προκύπτει ότι οι υποψήφιοι έχουν παρακολουθήσει τέσσερα τουλάχιστον μαθήματα, υποχρεωτικά ή κατ' επιλογή, Πληροφορικής ή γνώσης χειρισμού Η/Υ. Καθένα από τα τέσσερα αυτά μαθήματα μπορεί να έχει πραγματοποιηθεί στο πλαίσιο της απόκτησης είτε προπτυχιακού τίτλου [Πανεπιστημιακής (ΠΕ), ή Τεχνολογικής (ΤΕ) Εκπαίδευσης] είτε μεταπτυχιακού τίτλου είτε διδακτορικού διπλώματος και υπολογίζονται αθροιστικά.

Οι υποψήφιοι της Πανεπιστημιακής, Τεχνολογικής και Δευτεροβάθμιας Εκπαίδευσης αποδεικνύουν επαρκώς τη γνώση πληροφορικής ή χειρισμού Η/Υ, προσκομίζοντας μόνο **βεβαιώσεις τμημάτων ΑΕΙ και ΤΕΙ** με τις οποίες πιστοποιείται ότι παρακολούθησαν επιτυχώς, σε προπτυχιακό ή μεταπτυχιακό επίπεδο, **τέσσερα (4) εξαμηνιαία μαθήματα** τα οποία κατά την εκτίμηση του οικείου Τμήματος **εμπίπτουν στην περιοχή της Πληροφορικής ή του χειρισμού Η/Υ**.

Διευκρινίζεται ότι τίτλοι σπουδών ανώτερης αλλά και κατώτερης κατηγορίας από την κατηγορία για την οποία υποβάλλει αίτηση ο υποψήφιος, εφόσον πληρούν και τις λοιπές προϋποθέσεις εγκυρότητας, γίνονται δεκτοί, δεδομένου ότι αφενός οι εν λόγω τρόποι απόδειξης προβλέπονται από το προσοντολόγιο, αφετέρου οι σχετικοί τίτλοι και βεβαιώσεις υποβάλλονται για την απόδειξη της γνώσης πληροφορικής ή χειρισμού Η/Υ και όχι για τη διεκδίκηση θέσης ανώτερης ή κατώτερης κατηγορίας της προκηρυσσόμενης.

(4) Με Κρατικό Πιστοποιητικό Πληροφορικής (ΚΠΠ) του Υπουργείου Παιδείας και Θρησκευμάτων.

Σε περίπτωση που ο υποψήφιος έχει ολοκληρώσει με επιτυχία τις εξετάσεις αλλά το σχετικό πιστοποιητικό **δεν έχει ακόμη εκδοθεί**, γίνεται αποδεκτή η **βεβαίωση επιτυχίας στις εξετάσεις του Κρατικού Πιστοποιητικού Πληροφορικής που χορηγείται από το Υπουργείο Παιδείας και Θρησκευμάτων**. Αν ο υποψήφιος επιλεγεί στην ειδικότητα που επιδιώκει, πρέπει να προσκομίσει το πιστοποιητικό στο φορέα πρόσληψης ή ανάθεσης του έργου.

(5) Με πιστοποιητικό ή βεβαίωση αποφοίτησης από την Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ).

Η γνώση χειρισμού Η/Υ στα αντικείμενα: α) παρουσιάσεων και β) βάσεων δεδομένων αποδεικνύεται με πιστοποιητικά γνώσης πληροφορικής ή χειρισμού Η/Υ που εκδίδονται από τους πιστοποιημένους φορείς της ανωτέρω παραγράφου (1), εφόσον σ' αυτά περιλαμβάνονται τα εν λόγω αντικείμενα.

Η γνώση πληροφορικής ή χειρισμού Η/Υ στα αντικείμενα: α) επεξεργασίας κειμένων, β) υπολογιστικών φύλλων, γ) υπηρεσιών διαδικτύου, δ) παρουσιάσεων και ε) βάσεων δεδομένων αποδεικνύεται, πέραν των προαναφερομένων, και με <u>τίτλους σπουδών</u>, τριτοβάθμιας, μεταδευτεροβάθμιας ή δευτεροβάθμιας εκπαίδευσης, ειδικότητας Πληροφορικής ή γνώσης χειρισμού Η/Υ, όπως αυτοί αναφέρονται παρακάτω:

ΤΙΤΛΟΙ ΣΠΟΥΔΩΝ
ΤΡΙΤΟΒΑΘΜΙΑΣ – ΜΕΤΑΔ/ΒΑΘΜΙΑΣ & ΔΕΥΤΕΡΟΒΑΘΜΙΑΣ ΕΚΠΑΙΔΕΥΣΗΣ
ΓΙΑ ΤΗΝ ΑΠΟΔΕΙΞΗ ΓΝΩΣΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ Ή ΧΕΙΡΙΣΜΟΥ Η/Υ
όπως αυτοί προσδιορίζονται για τους κλάδους ΠΕ Πληροφορικής, ΤΕ Πληροφορικής και ΔΕ Πληροφορικής στους Πίνακες 1, 2 και 3 αντίστοιχα του Παραρτήματος Α΄ του ΠΔ 85/2022 (Α΄232)

Α) ΠΑΝΕΠΙΣΤΗΜΙΑΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ

Πτυχίο ή δίπλωμα:

- Πληροφορικής
- Εφαρμοσμένης Πληροφορικής
- Εφαρμοσμένης Πληροφορικής με κατεύθυνση: i) Εφαρμοσμένης Πληροφορικής ή ii) Διοίκησης Τεχνολογίας
- Εφαρμοσμένης Πληροφορικής - εισαγωγική κατεύθυνση Επιστήμης και Τεχνολογίας Υπολογιστών
- Εφαρμοσμένης Πληροφορικής - εισαγωγική κατεύθυνση Πληροφοριακά Συστήματα
- Πληροφορικής και Τηλεματικής
- Επιστήμης Υπολογιστών
- Πληροφορικής και Τηλεπικοινωνιών
- Επιστήμης και Τεχνολογίας Υπολογιστών
- Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών
- Πληροφορικής με εφαρμογές στην Βιοϊατρική
- Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων
- Ψηφιακών Συστημάτων
- Επιστημών και Πολιτισμού – Κατεύθυνση Η/Υ
- Μηχανικού Ηλεκτρονικών Υπολογιστών και Πληροφορικής
- Μηχανικού Πληροφορικής και Τηλεπικοινωνιών
- Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών
- Ηλεκτρολόγου Μηχανικού και Τεχνολογίας Υπολογιστών
- Ηλεκτρολόγου Μηχανικού και Μηχανικού Η/Υ
- Ηλεκτρονικής και Μηχανικών Υπολογιστών
- Ηλεκτρονικού Μηχανικού και Μηχανικού Υπολογιστών
- Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
- Μηχανικού Η/Υ Τηλεπικοινωνιών και Δικτύων
- Μηχανικών Πληροφορικής και Υπολογιστών
- Μηχανικού Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών
- Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων
- Τεχνολογιών Ψηφιακής Βιομηχανίας

Α.Ε.Ι. της ημεδαπής ή ακαδημαϊκά ισοδύναμος ή ισότιμος τίτλος αντίστοιχης ειδικότητας σχολών της αλλοδαπής.

Β) ΤΕΧΝΟΛΟΓΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ

Πτυχίο ή δίπλωμα:

- Πληροφορικής
- Εφαρμοσμένης Πληροφορικής και Πολυμέσων
- Τηλεπληροφορικής και Διοίκησης
- Διαχείρισης Πληροφοριών
- Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων
- Εφαρμογών Πληροφορικής στη Διοίκηση και στην Οικονομία
- Βιομηχανικής Πληροφορικής
- Γεωπληροφορικής και Τοπογραφίας
- Πληροφορικής και Επικοινωνιών
- Πληροφορικής και Τεχνολογίας Υπολογιστών
- Ηλεκτρονικών Υπολογιστικών Συστημάτων
- Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών
- Τηλεπικοινωνιών και Δικτύων Η/Υ
- Τηλεπικοινωνιακών Συστημάτων και Δικτύων
- Επιχειρησιακής Πληροφορικής
- Μηχανικών Πληροφορικής Τ.Ε.
- Μηχανικών Ηλεκτρονικών Υπολογιστικών Συστημάτων Τ.Ε.
- Διοίκησης Επιχειρήσεων με κατεύθυνση Διοίκηση Πληροφοριακών Συστημάτων

- Πολιτικών Μηχανικών Τ.Ε. και Μηχανικών Τοπογραφίας και Γεωπληροφορικής Τ.Ε. με κατεύθυνση Μηχανικών Τοπογραφίας και Γεωπληροφορικής Τ.Ε.
- Τ.Ε.Ι. της ημεδαπής ή ισότιμος τίτλος αντίστοιχης ειδικότητας σχολών της αλλοδαπής.

Γ) ΜΕΤΑΔΕΥΤΕΡΟΒΑΘΜΙΑΣ & ΔΕΥΤΕΡΟΒΑΘΜΙΑΣ ΕΚΠΑΙΔΕΥΣΗΣ

Πτυχίο ή δίπλωμα ή απολυτήριος τίτλος ειδικότητας:

- Τεχνικός Δικτύων και Τηλεπικοινωνιών
- Τεχνικός Η/Υ
- Τεχνικός Λογισμικού Η/Υ
- Τεχνικός Εφαρμογών Πληροφορικής (Πολυμέσα/Web Designer – Developer/Video Games)
- Ειδικός Εφαρμογών Πληροφορικής
- Προγραμματιστής Η/Υ
- Προγραμματιστής Βοηθός Αναλυτή Η/Υ
- Προγραμματιστής Βάσεων Δεδομένων
- Προγραμματιστής Εφαρμογών
- Πληροφορικής Εφαρμογών Πολυμέσων
- Τεχνικός Βιομηχανικού Λογισμικού
- Τεχνικός Τηλεπληροφορικής
- Τεχνικός Δικτύων
- Τεχνικός Εφαρμογών Ιατρικής Πληροφορικής
- Τεχνικός Εφαρμογών Πληροφορικής με Πολυμέσα (Multimedia)
- Ειδικός Εφαρμογών Πληροφορικής με Πολυμέσα – multimedia
- Προγραμματιστής Η/Υ- Πληροφορικής Πολυμέσων
- Τεχνικός Διαχείρισης Συστημάτων και Παροχής Υπηρεσιών Intranet-Internet
- Τεχνικός Δικτύων Υπολογιστών
- Τεχνικός Εφαρμογών Πληροφορικής
- Τεχνικός Εφαρμογών Πληροφορικής, Δικτύων και Αυτοματισμού Γραφείων
- Τεχνικός Η/Υ, Επικοινωνιών και Δικτύων
- Τεχνικός Συστημάτων Υπολογιστών
- Τεχνικός Τεχνολογίας Internet
- Τεχνικός Συστημάτων Ανοικτού Λογισμικού
- Τεχνικός Προγραμματισμού Παιχνιδιών και Ψυχαγωγικών Εφαρμογών (Video Games)
- Ηλεκτρονικών Υπολογιστικών Συστημάτων
- Υποστήριξης Συστημάτων & Δικτύων Υπολογιστών
- Υποστήριξης Συστημάτων και Εφαρμογών Υπολογιστών
- Υποστήριξη Συστημάτων-Εφαρμογών και Δικτύων Υπολογιστών
- Υποστήριξη Συστημάτων-Εφαρμογών και Δικτύων
- Υποστήριξη Συστημάτων-Εφαρμογών και Δικτύων Η/Υ
- Υποστήριξης Συστημάτων Υπολογιστών
- Ηλεκτρονικός Υπολογιστικών Συστημάτων και Δικτύου
- Ηλεκτρονικών Υπολογιστικών Συστημάτων και Δικτύων
- Προγραμματιστών Δευτεροβάθμιας Εκπαίδευσης
- Προγραμματιστών Ηλεκτρονικών Υπολογιστών
- Τεχνικός Η/Υ και Δικτύων Η/Υ
- Τεχνικός Εφαρμογών Λογισμικού
- Τεχνικός Ηλεκτρονικών και Υπολογιστικών Συστημάτων, Εγκαταστάσεων
- Τεχνικός Ηλεκτρονικών και Υπολογιστικών Συστημάτων, Εγκαταστάσεων, Δικτύων και Τηλεπικοινωνιών
- Τεχνικών Ηλεκτρονικών Υπολογιστών
- Ηλεκτρονικών Εγκαταστάσεων και Αυτοματισμού Τεχνικών Η/Υ
- Τεχνικών Ηλεκτρονικών Υπολογιστών (Τεχνικών Η/Υ)
- Τεχνικός Η/Υ και Ηλεκτρονικών Μηχανών Γραφείου
- Τεχνικός Ηλεκτρονικών Υπολογιστικών Συστημάτων και Αυτοματοποίησης Γραφείου

Επαγγελματικής Ειδικότητας, Εκπαίδευσης και Κατάρτισης επιπέδου 5 (Ι.Ε.Κ. ή Μεταλυκειακού Έτους - Τάξη Μαθητείας ΕΠΑ.Λ.) ή Επαγγελματικής Κατάρτισης επιπέδου μεταδευτεροβάθμιας επαγγελματικής

εκπαίδευσης Ι.Ε.Κ. ή Επαγγελματικού Λυκείου (ΕΠΑ.Λ.) ή Επαγγελματικής Ειδικότητας, Εκπαίδευσης και Κατάρτισης επιπέδου 4 ΕΠΑ.Λ. ή Τεχνικού Επαγγελματικού Εκπαιδευτηρίου (Τ.Ε.Ε.) Β΄ κύκλου σπουδών ή Τεχνικού Επαγγελματικού Λυκείου (Τ.Ε.Λ.) ή Τμήματος Ειδίκευσης Ενιαίου Πολυκλαδικού Λυκείου (Ε.Π.Λ.) ή Μέσης Τεχνικής Επαγγελματικής Σχολής Εργοδηγών (Ν.Δ. 580/1970) ή άλλος ισότιμος τίτλος σχολικής μονάδας της ημεδαπής ή αλλοδαπής, αντίστοιχης ειδικότητας.

ή

Πτυχίο ή δίπλωμα ή απολυτήριος τίτλος ειδικότητας:

- Τεχνιτών Υποστήριξης Συστημάτων Υπολογιστών
- Υποστήριξης Συστημάτων Υπολογιστών
- Υπαλλήλων Χειριστών Η/Υ
- Ηλεκτρονικών Υπολογιστικών Συστημάτων
- Ηλεκτρονικός Υπολογιστικών Μονάδων
- Ηλεκτρονικός Συσκευών-Εγκαταστάσεων και Υπολογιστικών Μονάδων
- Τεχνιτών Ηλεκτρονικών Συσκευών, Εγκαταστάσεων και Υπολογιστικών Μονάδων
- Αυτοματισμού-Ηλεκτρονικών υπολογιστών

Επαγγελματικής Σχολής (ΕΠΑ.Σ.) ν.3475/2006 ή Επαγγελματικής Σχολής (ΕΠΑ.Σ.) Μαθητείας ΟΑΕΔ ν.3475/2006 ή Επαγγελματικής Σχολής ΟΑΕΔ (ν.4763/2020) ή Επαγγελματικής Σχολής Κατάρτισης Ε.Σ.Κ. (ν.4763/2020) ή Σχολής Επαγγελματικής Κατάρτισης Σ.Ε.Κ. (ν.4186/2013) ή Τεχνικού Επαγγελματικού Εκπαιδευτηρίου Τ.Ε.Ε. Α΄ κύκλου σπουδών ή Τεχνικής Επαγγελματικής Σχολής Τ.Ε.Σ. (ν.1566/1985 ή ν.576/1997) ή Σχολής Μαθητείας ΟΑΕΔ (ν.1346/1983 ή ν.1566/1985) ή άλλος ισότιμος τίτλος σχολικής μονάδας της ημεδαπής ή αλλοδαπής, αντίστοιχης ειδικότητας.

13-06-2024

ΕΙΔΙΚΟ ΠΑΡΑΡΤΗΜΑ (Α2)
ΑΠΟΔΕΙΞΗΣ ΓΛΩΣΣΟΜΑΘΕΙΑΣ

Η γνώση ξένων γλωσσών αποδεικνύεται με τους εξής τρόπους:

- **Πιστοποιητικά γλωσσομάθειας**

Στον παρακάτω πίνακα αποτυπώνονται τα πιστοποιητικά γλωσσομάθειας που γίνονται αποδεκτά, ανά επίπεδο γνώσης της κάθε ξένης γλώσσας κατά τα αναφερόμενα στο Κοινό Ευρωπαϊκό Πλαίσιο Αναφοράς για τις γλώσσσες (CEFR), άριστο Γ2 ή C2, πολύ καλό Γ1 ή C1, καλό Β2 ή B2, μέτριο Β1 ή B1 και φορέα έκδοσης αυτών.

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	AIM Awards Level 3 Certificate in ESOL International (C2) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Awards Level 2 Certificate in ESOL International (C1) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Awards Level 1 Certificate in ESOL International (B2) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Awards Entry Level Certificate in ESOL International (Entry 3) (B1) (Ενότητες: Listening, Reading, Writing, Speaking)
	AIM Qualifications Level 3 Certificate in ESOL International (C2) (Anglia Mastery) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Qualifications Level 2 Certificate in ESOL International (C1) (Anglia Proficiency) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Qualifications Level 1 Certificate in ESOL International (B2) (Anglia Advanced) (Ενότητες: Listening, Reading, Writing, Speaking)	AIM Qualifications Entry Level Certificate in ESOL International (Entry 3) (B1) (Anglia Intermediate) (Ενότητες: Listening, Reading, Writing, Speaking)
	Ascentis Level 3 Certificate in ESOL International (CEF C2)	Ascentis Level 2 Certificate in ESOL International (CEF C1)	Ascentis Level 1 Certificate in ESOL International (CEF B2)	Ascentis Entry Level Certificate in ESOL International (Entry 3) CEF B1
	ADVANCED LEVEL CERTIFICATE IN ENGLISH (ALCE) του HELLENIC AMERICAN UNIVERSITY (Nashua, New Hampshire,USA) με συνολική βαθμολογία 74-100	ADVANCED LEVEL CERTIFICATE IN ENGLISH (ALCE) έως 31/12/2021 ή ADVANCED LEVEL CERTIFICATE IN ENGLISH (ALCE) με συνολική βαθμολογία 55-73 από 1/1/2022 του HELLENIC AMERICAN UNIVERSITY (Nashua, New Hampshire,USA)	-	-
	-	-	Assessment Board for Language Examinations: Level B2 (ABLE B2) του Hellenic American University (Nashua, New Hampshire, USA)	-

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	-	-	-	BASIC COMMUNICATION CERTIFICATE IN ENGLISH (BCCE) του HELLENIC AMERICAN UNIVERSITY (Nashua, New Hampshire,USA)
	BULATS English Language Test, βαθμολογία 90-100, του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH (Για πιστοποιητικά που έχουν εκδοθεί έως και 19/11/2019)	BULATS English Language Test, βαθμολογία 75-89, του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH (Για πιστοποιητικά που έχουν εκδοθεί έως και 19/11/2019)	BULATS English Language Test, βαθμολογία 60-74, του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH (Για πιστοποιητικά που έχουν εκδοθεί έως και 19/11/2019)	BULATS English Language Test, βαθμολογία 40-59, του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH (Για πιστοποιητικά που έχουν εκδοθεί έως και 19/11/2019)
	-	BUSINESS ENGLISH CERTIFICATE – HIGHER (BEC HIGHER) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH	BUSINESS ENGLISH CERTIFICATE – VANTAGE (BEC VANTAGE) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH	BUSINESS ENGLISH CERTIFICATE - PRELIMINARY (BEC PRELIMINARY) (UNIVERSITY OF CAMBRIDGE LOCAL EXAMINATIONS SYNDICATE (UCLES) ή CAMBRIDGE ASSESSMENT ENGLISH
	BUSINESS ENGLISH CERTIFICATE HIGHER του CAMBRIDGE ASSESSMENT ENGLISH overall score 200-210	BUSINESS ENGLISH CERTIFICATE HIGHER του CAMBRIDGE ASSESSMENT ENGLISH overall score 180-199	BUSINESS ENGLISH CERTIFICATE PRELIMINARY του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-170	BUSINESS ENGLISH CERTIFICATE PRELIMINARY του CAMBRIDGE ASSESSMENT ENGLISH overall score 140-159.
	-	BUSINESS ENGLISH CERTIFICATE VANTAGE του CAMBRIDGE ASSESSMENT ENGLISH overall score 180-190	BUSINESS ENGLISH CERTIFICATE VANTAGE του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179	BUSINESS ENGLISH CERTIFICATE VANTAGE του CAMBRIDGE ASSESSMENT ENGLISH overall score 140-159
	CERTIFICATE IN ADVANCED ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 200-210	CERTIFICATE IN ADVANCED ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 180-199	CERTIFICATE IN ADVANCED ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179	-
	CERTIFICATE OF PROFICIENCY IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 200-230	CERTIFICATE OF PROFICIENCY IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 180-199	-	-
	CERTIFICATE OF PROFICIENCY IN ENGLISH του Πανεπιστημίου	CERTIFICATE IN ADVANCED ENGLISH του Πανεπιστημίου	FIRST CERTIFICATE IN ENGLISH του Πανεπιστημίου CAMBRIDGE ή του	PRELIMINARY ENGLISH TEST (PET) του Πανεπιστημίου CAMBRIDGE ή του

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH	CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH	CAMBRIDGE ASSESSMENT ENGLISH	CAMBRIDGE ASSESSMENT ENGLISH
ΑΓΓΛΙΚΑ	-	FIRST CERTIFICATE IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 180-190	FIRST CERTIFICATE IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179	FIRST CERTIFICATE IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 140-159
	ISE IV INTEGRATED SKILLS IN ENGLISH LEVEL 3 CERTIFICATE IN ESOL INTERNATIONAL του TRINITY COLLEGE LONDON	CERTIFICATE IN INTEGRATED SKILLS IN ENGLISH ISE III του TRINITY COLLEGE LONDON	CERTIFICATE IN INTEGRATED SKILLS IN ENGLISH ISE II του TRINITY COLLEGE LONDON	CERTIFICATE IN INTEGRATED SKILLS IN ENGLISH ISE I του TRINITY COLLEGE LONDON
	CITY & GUILDS LEVEL 3 CERTIFICATE IN ESOL INTERNATIONAL (reading, writing and listening) - MASTERY- **και** CITY & GUILDS LEVEL 3 CERTIFICATE IN ESOL INTERNATIONAL (Spoken) - MASTERY- (Συνυποβάλλονται αθροιστικά για την απόδειξη της άριστης γνώσης)	CITY & GUILDS LEVEL 2 CERTIFICATE IN ESOL INTERNATIONAL (reading, writing and listening) - EXPERT- **και** CITY & GUILDS LEVEL 2 CERTIFICATE IN ESOL INTERNATIONAL (Spoken) - EXPERT- (Συνυποβάλλονται αθροιστικά για την απόδειξη της πολύ καλής γνώσης)	CITY & GUILDS LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (reading, writing and listening) - COMMUNICATOR- **και** CITY & GUILDS LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (Spoken) - COMMUNICATOR- (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης)	CITY & GUILDS ENTRY LEVEL CERTIFICATE IN ESOL INTERNATIONAL (reading, writing and listening) (ENTRY 3) - ACHIEVER- **και** CITY & GUILDS ENTRY LEVEL CERTIFICATE IN ESOL INTERNATIONAL (Spoken) (ENTRY 3) - ACHIEVER - (Συνυποβάλλονται αθροιστικά για την απόδειξη της μέτριας γνώσης)
	CITY & GUILDS CERTIFICATE IN INTERNATIONAL ESOL-MASTERY **και** CITY & GUILDS CERTIFICATE IN INTERNATIONAL SPOKEN ESOL - MASTERY- (Συνυποβάλλονται αθροιστικά για την απόδειξη της άριστης γνώσης)	CITY & GUILDS CERTIFICATE IN INTERNATIONAL ESOL - EXPERT- **και** CITY & GUILDS CERTIFICATE IN INTERNATIONAL SPOKEN ESOL - EXPERT - (Συνυποβάλλονται αθροιστικά για την απόδειξη της πολύ καλής γνώσης)	CITY & GUILDS CERTIFICATE IN INTERNATIONAL ESOL - COMMUNICATOR - **και** CITY & GUILDS CERTIFICATE IN INTERNATIONAL SPOKEN ESOL - COMMUNICATOR - (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης)	CITY & GUILDS CERTIFICATE IN INTERNATIONAL ESOL - ACHIEVER - **και** CITY & GUILDS CERTIFICATE IN INTERNATIONAL SPOKEN ESOL - ACHIEVER- (Συνυποβάλλονται αθροιστικά για την απόδειξη της μέτριας γνώσης)

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	ECPE- CERTIFICATE OF PROFICIENCY IN ENGLISH του Πανεπιστημίου MICHIGAN (ENGLISH LANGUAGE INSTITUTE ή Cambridge Michigan Language Assessments - CaMLA ή Michigan Language Assessment)	-	(ECCE)- CERTIFICATE OF COMPETENCY IN ENGLISH του Πανεπιστημίου MICHIGAN (ENGLISH LANGUAGE INSTITUTE ή Cambridge Michigan Language Assessments - CaMLA ή Michigan Language Assessment)	-
	EDI Level 3 Certificate in ESOL International JETSET Level 7 (CEF C2)	EDI Level 2 Certificate in ESOL International JETSET Level 6 (CEF C1)	EDI Level 1 Certificate in ESOL International JETSET Level 5 (CEF B2)	EDI Entry Level Certificate in ESOL International (Entry Level 3) JETSET Level 4 (CEF B1)
	ESB Level 3 Certificate in ESOL International All Modes (Council of Europe Level C2)	ESB Level 2 Certificate in ESOL International All Modes (Council of Europe Level C1)	ESB Level 1 Certificate in ESOL International All Modes (Council of Europe Level B2)	ESB Entry Level Certificate in ESOL International All Modes (entry 3) (Council of Europe Level B1)
	INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH – The British Council – IDP Education Australia IELTS Australia με βαθμολογία από 8,5 και άνω	INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH – The British Council – IDP Education Australia IELTS Australia με βαθμολογία από 7 έως 8	INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH – The British Council – IDP Education Australia IELTS Australia με βαθμολογία από 5,5 έως 6,5	INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) από το University of Cambridge Local Examinations Syndicate (UCLES) – The British Council-IDP Education Australia με βαθμολογία από 4 έως 5
	GA Level 3 Certificate in ESOL International – CEFR: C2	GA Level 2 Certificate in ESOL International – CEFR: C1	GA Level 1 Certificate in ESOL International – CEFR: B2	GA Entry Level Certificate in ESOL International (Entry 3) (CEFR: B1)
	GA Level 3 Certificate in ESOL International (Classic C2)	GA Level 2 Certificate in ESOL International (Classic C1)	GA Level 1 Certificate in ESOL International (Classic B2)	GA Entry Level 1 Certificate in ESOL International (Classic B1)
	-	-	-	KEY ENGLISH TEST του CAMBRIDGE ASSESSMENT ENGLISH overall score 140-150
	C2- LanguageCert Level 3 Certificate in ESOL International (Listening, Reading, Writing)	C1- LanguageCert Level 2 Certificate in ESOL International (Listening, Reading, Writing) (Expert C1) **και** C1 -	B2- LanguageCert Level 1 Certificate in ESOL International (Listening, Reading, Writing) (Communicator B2)	B1- LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Listening, Reading, Writing) (Achiever B1) **και** B1-

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	(MasteryC2) **και** C2- LanguageCert Level 3 Certificate in ESOL International (Speaking) (Mastery C2) (Συνυποβάλλονται αθροιστικά για την απόδειξη της άριστης γνώσης)	LanguageCert Level 2 Certificate in ESOL International (Speaking) (Expert C1) (Συνυποβάλλονται αθροιστικά για την απόδειξη της πολύ καλής γνώσης)	**και** B2 - LanguageCert Level 1 Certificate in ESOL International (Speaking) (Communicator B2) (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης)	LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Speaking) (Achiever B1) (Συνυποβάλλονται αθροιστικά για την απόδειξη της μέτριας γνώσης)
ΑΓΓΛΙΚΑ	LanguageCert Test of English (LTE) - LanguageCert Level 3 Certificate in ESOL International (Listening, Reading) (LanguageCert Test of English C2) (μέχρι 30.06.2024)*	LanguageCert Test of English (LTE) - LanguageCert Level 2 Certificate in ESOL International (Listening, Reading) (LanguageCert Test of English C1) (μέχρι 30.06.2024)*	LanguageCert Test of English (LTE) - LanguageCert Level 1 Certificate in ESOL International (Listening, Reading) (LanguageCert Test of English B2) (μέχρι 30.06.2024)*	LanguageCert Test of English (LTE) - LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Listening, Reading) (LanguageCert Test of English B1) (μέχρι 30.06.2024)*
	LanguageCert Level 3 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Test of English C2)	LanguageCert Level 2 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Test of English C1)	LanguageCert Level 1 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Test of English B2)	LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Listening, Reading, Writing, Speaking) (LanguageCert Test of English B1)
	LanguageCert Level 3 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Academic C2)	LanguageCert Level 2 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Academic C1)	LanguageCert Level 1 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert Academic B2)	LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Listening, Reading, Writing, Speaking) (LanguageCert Academic B1)
	-	LanguageCert Level 2 Certificate in ESOL International (Listening, Reading, Writing, Speaking) (LanguageCert General C1)	LanguageCert Level 1 Certificate in ESOL (Listening, Reading, Writing, Speaking) (LanguageCert General B2)	LanguageCert Entry Level Certificate in ESOL International (Entry 3) (Listening, Reading, Writing, Speaking) (LanguageCert General B1)
	LONDON TESTS OF ENGLISH LEVEL 5 - PROFICIENT COMMUNICATION - του EDEXCEL	LONDON TESTS OF ENGLISH LEVEL 4 - ADVANCED COMMUNICATION- του EDEXCEL	LONDON TESTS OF ENGLISH LEVEL 3 - UPPER INTERMEDIATE COMMUNICATION- του EDEXCEL	LONDON TESTS OF ENGLISH LEVEL 2 – INTERMEDIATE COMMUNICATION-του EDEXCEL
	EDEXCEL LEVEL 3 CERTIFICATE IN ESOL INTERNATIONAL (CEF C2)	EDEXCEL LEVEL 2 CERTIFICATE IN ESOL INTERNATIONAL (CEF C1)	EDEXCEL LEVEL I CERTIFICATE IN ESOL INTERNATIONAL (CEF B2)	EDEXCEL ENTRY LEVEL CERTIFICATE IN ESOL INTERNATIONAL (ENTRY 3) (CEF B1)
	LRN Level 3 Certificate in ESOL International (CEF C2)	LRN Level 2 Certificate in ESOL International (CEF C1)	LRN Level 1 Certificate in ESOL International (CEF B2)	LRN Entry Level Certificate in ESOL International (Entry 3) (CEF B1)

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	-	MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, Speaking) βαθμολογία από 190 έως 240 του Michigan Language Assessment ή CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS-CaMLA (μέχρι 30.06.2024)*	MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, Speaking) βαθμολογία από 157 έως 189 του Michigan Language Assessment ή CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS-CaMLA (μέχρι 30.06.2024)*	MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, Speaking) βαθμολογία από 120 έως 156 του Michigan Language Assessment ή CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS-CaMLA (μέχρι 30.06.2024)*
	-	MET- MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, μέχρι 30.06.2024* ή Ενότητες: Listening, Reading, Speaking, Writing) βαθμολογία από 64 έως 80 του Michigan Language Assessment	MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, μέχρι 30.06.2024* ή Ενότητες: Listening, Reading, Speaking, Writing) βαθμολογία από 53 έως 63 του Michigan Language Assessment	MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, μέχρι 30.06.2024* ή Ενότητες: Listening, Reading, Speaking, Writing) βαθμολογία από 40 έως 52 του Michigan Language Assessment
	-	MICHIGAN ENGLISH LANGUAGE ASSESSMENT BATTERY (MELAB) βαθμολογία από 91 έως 99 του CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS (CaMLA) ή του MICHIGAN LANGUAGE ASSESSMENT	MICHIGAN ENGLISH LANGUAGE ASSESSMENT BATTERY (MELAB) βαθμολογία από 80 έως 90 του CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS ή του MICHIGAN LANGUAGE ASSESSMENT	MICHIGAN ENGLISH LANGUAGE ASSESSMENT BATTERY (MELAB) βαθμολογία από 67 έως 79 του CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS ή του MICHIGAN LANGUAGE ASSESSMENT
	Michigan State University – Certificate of English Language Proficiency (MSU – CELP): CEF C2	-	Michigan State University – Certificate of English Language Competency (MSU – CELC): CEF B2	-
	NOCN Level 3 Certificate in ESOL International (C2)	NOCN Level 2 Certificate in ESOL International (C1)	NOCN Level 1 Certificate in ESOL International (B2)	NOCN Entry Level Certificate in ESOL International (Entry 3) (B1)
	NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level C2	NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level C1	NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level B2	NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level B1
	OCNLR Level 3 Certificate in ESOL International (CEFR C2)	OCNLR Level 2 Certificate in ESOL International (CEFR C1)	OCNLR Level 1 Certificate in ESOL International (CEFR B2)	OCNLR Entry Level Certificate in ESOL International (Entry 3) (CEFR B1)

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	OCNW Certificate in ESOL International at Level 3 (Common European Framework equivalent level C2) (μέχρι 31/8/2009)	OCNW Certificate in ESOL International at Level 2 (Common European Framework equivalent level C1) (μέχρι 31/8/2009)	OCNW Certificate in ESOL International at Level 1 (Common European Framework equivalent level B2) (μέχρι 31/8/2009)	OCNW Certificate in ESOL International at Entry Level 3 (Common European Framework equivalent level B1) (μέχρι 31/8/2009)
	Open College Network West Midlands Level 3 Certificate in ESOL International (CEFR C2)	Open College Network West Midlands Level 2 Certificate in ESOL International (CEFR C1)	Open College Network West Midlands Level 1 Certificate in ESOL International (CEFR B2)	Open College Network West Midlands Entry Level Certificate in ESOL International (Entry 3) (CEFR B1)
	PEARSON EDI Level 3 Certificate in ESOL International (CEF C2)	PEARSON EDI Level 2 Certificate in ESOL International (CEF C1)	PEARSON EDI Level 1 Certificate in ESOL International (CEF B2)	PEARSON EDI Entry 3 Certificate in ESOL International (CEF B1)
	PEARSON LCCI LEVEL 3 CERTIFICATE IN ESOL INTERNATIONAL (CEFR C2)	PEARSON LCCI LEVEL 2 CERTIFICATE IN ESOL INTERNATIONAL (CEFR C1)	PEARSON LCCI LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (CEFR B2)	PEARSON LCCI ENTRY 3 CERTIFICATE IN ESOL INTERNATIONAL (CEFR B1)
	PEARSON TEST OF ENGLISH GENERAL LEVEL 5 -PROFICIENT COMMUNICATION - του EDEXCEL	PEARSON TEST OF ENGLISH GENERAL LEVEL 4 - ADVANCED COMMUNICATION - του EDEXCEL	PEARSON TEST OF ENGLISH GENERAL LEVEL 3 UPPER-INTERMEDIATE COMMUNICATION - του EDEXCEL	PEARSON TEST OF ENGLISH GENERAL LEVEL 2- INTERMEDIATE COMMUNICATION - του EDEXCEL
	PEARSON EDEXCEL Level 3 Certificate in ESOL International (CEF C2) (ENGLISH International Certificate)	PEARSON EDEXCEL LEVEL 2 CERTIFICATE IN ESOL INTERNATIONAL (CEF C1) (ENGLISH INTERNATIONAL CERTIFICATE)	PEARSON EDEXCEL LEVEL I CERTIFICATE IN ESOL INTERNATIONAL (CEF B2) (ENGLISH INTERNATIONAL CERTIFICATE)	PEARSON EDEXCEL ENTRY LEVEL CERTIFICATE IN ESOL INTERNATIONAL (ENTRY 3) (CEF B1) (ENGLISH INTERNATIONAL CERTIFICATE)
	PEARSON LCCI EFB LEVEL 4 (Ενότητες: Reading, Writing, Listening, Speaking, με βαθμό “Distinction” ή “Credit”)	PEARSON LCCI EFB LEVEL 4 (Ενότητες: Reading, Writing, Listening, Speaking, σε περίπτωση που η μία εκ των ενοτήτων είναι με βαθμό “Pass”)	PEARSON LCCI EFB LEVEL 3 (Ενότητες: Reading, Writing, Listening, Speaking, σε περίπτωση που η μία εκ των ενοτήτων είναι με βαθμό “Pass”)	PEARSON LCCI EFB LEVEL 2 (Ενότητες: Reading, Writing, Listening, Speaking, σε περίπτωση που η μία εκ των ενοτήτων είναι με βαθμό “Pass”)
	-	PEARSON LCCI EFB LEVEL 3 (Ενότητες: Reading, Writing, Listening, Speaking, με βαθμό “Distinction” ή “Credit”)	PEARSON LCCI EFB LEVEL 2 (Ενότητες: Reading, Writing, Listening, Speaking, με βαθμό “Distinction” ή “Credit”)	PEARSON LCCI EFB Level 1 (Ενότητες: Reading, Writing, Listening, Speaking, με βαθμό “Distinction” ή “Credit”)
	-	-	PRELIMINARY ENGLISH TEST του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-170	PRELIMINARY ENGLISH TEST του CAMBRIDGE ASSESSMENT ENGLISH overall score 140-159

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΑΓΓΛΙΚΑ	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC Listening, Reading) του EDUCATIONAL TESTING SERVICE/ CHAUNCEY, USA, βαθμολογία από 1/12/2019 από 925 έως 990 (μέχρι 30.06.2024)*	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC Listening, Reading) του EDUCATIONAL TESTING SERVICE/ CHAUNCEY, USA, βαθμολογία από 785 έως 900 και από 1/12/2019 βαθμολογία από 785 έως 920 (μέχρι 30.06.2024)*	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC Listening, Reading) του EDUCATIONAL TESTING SERVICE/ CHAUNCEY, USA, βαθμολογία από 505 έως 780 (μέχρι 30.06.2024)*	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC Listening, Reading) του EDUCATIONAL TESTING SERVICE/ CHAUNCEY, USA, βαθμολογία από 405 έως 500 (μέχρι 30.06.2024)*
	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION -TOEIC 4-Skills (Listening, Reading, Speaking, Writing) του EDUCATIONAL TESTING SERVICE (ETS), Level C2	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION - TOEIC 4-Skills (Listening, Reading, Speaking, Writing) του EDUCATIONAL TESTING SERVICE (ETS), Level C1	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION - TOEIC 4-Skills (Listening, Reading, Speaking, Writing) του EDUCATIONAL TESTING SERVICE (ETS), Level B2	TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION - TOEIC 4-Skills (Listening, Reading, Speaking, Writing) του EDUCATIONAL TESTING SERVICE (ETS), Level B1
	Test of Interactive English, C2 Level (ACELS)	Test of Interactive English, C1 Level (ACELS)	Test of Interactive English, B2 Level (ACELS)	Test of Interactive English, B1 Level (ACELS)
	Test of Interactive English, C2 Level (Gatehouse Awards)	Test of Interactive English, C1 Level (Gatehouse A wards).	Test of Interactive English, B2 Level (Gatehouse Awards)	Test of Interactive English, B1 Level (Gatehouse Awards)
	-	Test of Interactive English, C1 + Level (ACELS)	Test of Interactive English, B2 + Level (ACELS)	Test of Interactive English, B1 + Level (ACELS)
	VTCT (ITEC) Level 3 Certificate in ESOL International (C2)	VTCT (ITEC) Level 2 Certificate in ESOL International (C1)	VTCT (ITEC) Level 1 Certificate in ESOL International (B2)	VTCT (ITEC) Entry Level Certificate in ESOL International (Entry 3) (B1)
	Κρατικό πιστοποιητικό γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό πιστοποιητικό γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003
	*** Για τα πιστοποιητικά που έχουν εκδοθεί ή πρόκειται να εκδοθούν μέχρι και τις 30.06.2024 (άρθρο 115 του ν. 5079/2023).**			
ΓΑΛΛΙΚΑ	D.A.L.F. – OPTION LETTRES ή DALF C2 Γαλλικό Υπουργείο Παιδείας - CIEP	DELF 2ND DEGRE (UNITES A5 ET A6) ή DALF C1 Γαλλικό Υπουργείο Παιδείας - CIEP	DELF 1ER DEGRE (UNITES A1, A2, A3, A4) ή DELF B2 Γαλλικό Υπουργείο Παιδείας - CIEP	DELF B1 Γαλλικό Υπουργείο Παιδείας - CIEP
	DIPLOME DE LANGUE ET LITTERATURE FRANCAISES (SORBONNE II) [Μέχρι το 1999 ο	-	-	-

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	τίτλος του διπλώματος ήταν: DIPLOME D' ETUDES FRANCAISES (SORBONNE II) Paris-Sorbonne Universite]			
ΓΑΛΛΙΚΑ	DIPLOME SUPERIEUR D' ETUDES FRANCAISES (SORBONNE 3EME DEGRE) Paris-Sorbonne Universite	CERTIFICAT PRATIQUE DE LANGUE FRANCAISE SORBONNE I ή (Paris-Sorbonne C1) Paris-Sorbonne Universite	CERTIFICAT PRATIQUE DE LANGUE FRANCAISE-SORBONNE B2 Paris-Sorbonne Universite	CERTIFICAT INTERMEDIAIRE DE LANGUE FRANCAISE-PARIS- SORBONNE B1 Paris-Sorbonne Universite
	-	DIPLOME D' ETUDES SUPERIEURES (DES) (χορηγείτο μέχρι το1996) - Γαλλικό Ινστιτούτο Ελλάδος	CERTIFICAT DE LANGUE FRANCAISE (το οποίο χορηγείτο μέχρι το 1996) Γαλλικό Ινστιτούτο Ελλάδος.	-
	Δίπλωμα ALLIANCE FRANCAISE.	-	-	-
	Certificat de competences linguistiques του Institut Superieur des Langues Vivantes (ISLV), Departement de francais, του Πανεπιστημίου της Λιέγης – Επίπεδο C2	Certificat de competences linguistiques του Institut Superieur des Langues Vivantes (ISLV), Departement de francais, του Πανεπιστημίου της Λιέγης – Επίπεδο C1	Certificat de competences linguistiques του Institut Superieur des Langues Vivantes (ISLV), Departement de francais, του Πανεπιστημίου της Λιέγης – Επίπεδο B2	Certificat de competences linguistiques του Institut Superieur des Langues Vivantes (ISLV), Departement de francais, του Πανεπιστημίου της Λιέγης – Επίπεδο B1
	CERTIFICAT V.B.L.T. NIVEAU PROFESSIONNEL του Πανεπιστημίου Γενεύης	CERTIFICAT V.B.L.T. NIVEAU OPERATIONNEL του Πανεπιστημίου Γενεύης	CERTIFICAT V.B.L.T. NIVEAU SOCIAL του Πανεπιστημίου Γενεύης	CERTIFICAT V.B.L.T. NIVEAU SURVIE του Πανεπιστημίου της Γενεύης
	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν.3149/2003.
	Για τα πιστοποιητικά παλαιότερων ετών τα οποία δεν αναγράφονται, απαιτείται βεβαίωση, από τον οικείο φορέα (Γαλλικό Ινστιτούτο Αθηνών-Υπηρεσία Εξετάσεων), για το επίπεδο του πιστοποιητικού.			
ΓΕΡΜΑΝΙΚΑ	Goethe-Zertifikat C2: Großes Deutsches Sprachdiplom (Ενότητες: Lesen, Hören, Schreiben, Sprechen) του Ινστιτούτου Goethe.	GOETHE – ZERTIFIKAT C1 του Ινστιτούτου Goethe.	GOETHE – ZERTIFIKAT B2 (Ενότητες: Lesen, Hören, Schreiben, Sprechen) του Ινστιτούτου Goethe.	Goethe-Zertifikat B1 (Ενότητες: Lesen, Hören, Schreiben, Sprechen) του Ινστιτούτου Goethe.

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	GROSSES DEUTSCHES SPRACHDIPLOM (GDS), του Πανεπιστημίου Ludwig-Maximilian του Μονάχου και του Ινστιτούτου Goethe (μέχρι 31-12-2011)	-	ZERTIFIKAT DEUTSCH FUR DEN BERUF (ZDfB) του Ινστιτούτου Goethe	ZERTIFIKAT DEUTSCH (ZD) του Ινστιτούτου Goethe (μέχρι 31-7-2013)
ΓΕΡΜΑΝΙΚΑ	KLEINES DEUTSCHES SPRACHDIPLOM (KDS), του Πανεπιστημίου Ludwig-Maximilian του Μονάχου και του Ινστιτούτου Goethe (μέχρι 31-12-2011)	-	-	-
	ZENTRALE OBERSTUFENPRUFUNG (ZOP) του Ινστιτούτου Goethe (μέχρι 31-12-2011)	ZENTRALE MITTELSTUFENPRUFUNG (ZMP) (μέχρι 2007) του Ινστιτούτου Goethe.	-	-
	ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT C2. (Ενότητες: Lesen, Hören, Schreiben, Sprechen)	ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) C1 OBERSTUFE DEUTSCH (μέχρι 31/12/2014)	ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) B2 MITTELSTUFE DEUTSCH (μέχρι 31/12/2014)	ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD)B1 ZERTIFIKAT DEUTSCH (μέχρι 31/12/2013)
	-	(Από 1/1/2015) ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT C1	(Από 1/1/2015) ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT B2	(Από 1/1/2014) ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT B1 (Ενότητες: Lesen, Hören, Schreiben, Sprechen)
	-	(Από 1/1/2018) ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT C1 (ENOTHTA 1: LESEN, HOREN, SCHREIBEN, ENOTHTA 2: SPRECHEN)	(Από 1/1/2018) ÖSTERREICHISCHES SPRACHDIPLOM (ÖSD) ZERTIFIKAT B2 (ENOTHTA 1: LESEN, HOREN, SCHREIBEN, ENOTHTA 2: SPRECHEN)	-
	-	PRUFUNG WIRTSCHAFTSDEUTSCH (PWD) του Ινστιτούτου Goethe.	-	-
	-	-	-	ZERTIFIKAT DEUTSCH ALS FREMDSPRACHE (ZDAF) του Ινστιτούτου GOETHE [(Αντικαταστάθηκε από την 1-1-2000 (στην Ελλάδα από τον Μάιο του 2000)] με το ZERTIFIKAT

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
				DEUTSCH (ZD).
	ZERTIFIKAT V.B.L.T. PROFESSIONALES LEBEN του Πανεπιστημίου Γενεύης	ZERTIFIKAT V.B.L.T. SELBSTÄNDIGES LEBEN του Πανεπιστημίου Γενεύης	ZERTIFIKAT V.B.L.T. SOZIALES LEBEN του Πανεπιστημίου Γενεύης	ZERTIFIKAT V.B.L.T. ALTAGLICHES LEBEN του Πανεπιστημίου της Γενεύης
	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν.3149/2003.
ΙΤΑΛΙΚΑ	CERTIFICATO DI CONOSCENZA DELLA LINGUA ITALIANA, LIVELLO 5 (CELI 5) του Πανεπιστημίου της Περούντζια.	CERTIFICATO DI CONOSCENZA DELLA LINGUA ITALIANA LIVELLO 4 (CELI 4) του Πανεπιστημίου της Περούντζια.	CERTIFICATO DI CONOSCENZA DELLA LINGUA ITALIANA LIVELLO 3 (CELI 3) του Πανεπιστημίου της Περούντζια.	CERTIFICATO DI CONOSCENZA DELLA LINGUA ITALIANA, LIVELLO 2 (CELI 2) του Πανεπιστημίου της Περούντζια.
	DIPLOMA DI LINGUA E CULTURA ITALIANA (του Ιταλικού Μορφωτικού Ινστιτούτου Αθηνών)	DIPLOMA DI LINGUA ITALIANA (του Ιταλικού Μορφωτικού Ινστιτούτου Αθήνας έως τον Ιούνιο 2014)	DIPLOMA DI LINGUA ITALIANA (Ιταλικό Μορφωτικό Ινστιτούτο Θεσσαλονίκης και Αθήνας)	-
	DIPLOMA DI TRADUTTORE ή DIPLOMA DEL CORSO SUPERIORE DI TRADUTTORE	-	-	-
	DIPLOMA SUPERIORE DI LINGUA E CULTURA ITALIANA	DIPLOMA AVANZATO DI LINGUA ITALIANA	-	DIPLOMA INTERMEDIO DI LINGUA ITALIANA
	P.L.I.D.A. C2 ή P.L.I.D.A. D (έως το 2003)	P.L.I.D.A. C1 ή P.L.I.D.A. C (έως το 2003)	P.L.I.D.A. B2 ή P.L.I.D.A. B (έως το 2003)	P.L.I.D.A. B1
	CERTIFICATO V.B.L.T. LIVELLO PROFESSIONALE του Πανεπιστημίου Γενεύης	CERTIFICATO V.B.L.T. LIVELLO OPERATIVO του Πανεπιστημίου Γενεύης	CERTIFICATO V.B.L.T. LIVELLO SOCIALLE του Πανεπιστημίου Γενεύης	CERTIFICATO V.B.L.T. LIVELLO SUPRAWIVENZA του Πανεπιστημίου Γενεύης
	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν.3149/2003.

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	v.3149/2003.	v.3149/2003.	v.3149/2003.	
	Για τα πιστοποιητικά παλαιοτέρων ετών που έχουν χορηγηθεί από το Ιταλικό Μορφωτικό Ινστιτούτο (Αθήνας και Θεσσαλονίκης) και δεν αναγράφονται, απαιτείται βεβαίωση, από τον οικείο φορέα (Ιταλικό Μορφωτικό Ινστιτούτο Αθηνών-Υπηρεσία Εξετάσεων), για το επίπεδο του πιστοποιητικού.			
ΙΣΠΑΝΙΚΑ	DIPLOMA DELE SUPERIOR DE ESPANOL (DELE) (μέχρι 2002)	-	DIPLOMA BASICO DE ESPANOL COMO LENGUA EXTRANJERA (DELE) (μέχρι 2002) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	CERTIFICADO INICIAL DE ESPANOL COMO LENGUA EXTRANJERA (DELE) (μέχρι 2002) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας
	DIPLOMA DE ESPANOL COMO LENGUA EXTRANJERA (NIVEL SUPERIOR) - (DELE) (μέχρι 2008)	-	DIPLOMA DE ESPANOL COMO LENGUA EXTRANJERA (NIVEL INTERMEDIO) - (DELE) (μέχρι 2008) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	DIPLOMA DE ESPANOL COMO LENGUA EXTRANJERA (NIVEL INICIAL) (DELE) (μέχρι 2008) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας
	CERTIFICADO SUPERIOR E.O.I. (ESCUELAS OFICIALES DE IDIOMAS) από το Υπουργείο Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	CERTIFICADO ELEMENTAL E.O.I. (ESCUELAS OFICIALES DE IDIOMAS)	-	
	DIPLOMA DE ESPANOL- NIVEL C2 (DELE) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	DIPLOMA DE ESPANOL-NIVEL C1 (DELE) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	DIPLOMA DE ESPANOL-NIVEL B2 (DELE) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας	DIPLOMA DE ESPANOL -NIVEL B1 (DELE) από το Ινστιτούτο Cervantes εξ ονόματος του Υπουργείου Παιδείας, Πολιτισμού και Αθλητισμού της Ισπανίας
	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν. 3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν. 3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν. 3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ. 19 του άρθρου 13 του ν. 3149/2003

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
ΡΩΣΙΚΑ	ΣΕΡΤΙΦΙΚΑΤ – РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ ЧЕТВЁРТЫЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ του Φιλολογικού Τμήματος του Κρατικού Πανεπιστημίου της Μόσχας «M.V. Lomonosov», με φορέα χορήγησης στην Ελλάδα το Ρωσικό Επιστημονικό και Πολιτιστικό Κέντρο της Πρεσβείας της Ρωσίας στην Ελλάδα (έως 31/12/2014)	ΣΕΡΤΙΦΙΚΑΤ – РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ ТРЕТИЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ του Φιλολογικού Τμήματος του Κρατικού Πανεπιστημίου της Μόσχας «M.V. Lomonosov», με φορέα χορήγησης στην Ελλάδα το Ρωσικό Επιστημονικό και Πολιτιστικό Κέντρο της Πρεσβείας της Ρωσίας στην Ελλάδα (έως 31/12/2014)	ΣΕΡΤΙΦΙΚΑΤ – РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ ВТОРОЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ του Φιλολογικού Τμήματος του Κρατικού Πανεπιστημίου της Μόσχας «M.V. Lomonosov», με φορέα χορήγησης στην Ελλάδα το Ρωσικό Επιστημονικό και Πολιτιστικό Κέντρο της Πρεσβείας της Ρωσίας στην Ελλάδα (έως 31/12/2014)	ΣΕΡΤΙΦΙΚΑΤ – РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ ПЕРВЫЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ του Φιλολογικού Τμήματος του Κρατικού Πανεπιστημίου της Μόσχας «M.V. Lomonosov», με φορέα χορήγησης στην Ελλάδα το Ρωσικό Επιστημονικό και Πολιτιστικό Κέντρο της Πρεσβείας της Ρωσίας στην Ελλάδα (έως 31/12/2014)
	ΣΕΡΤΙΦΙΚΑΤ Ο ΠΡΟΧΟΖΔΕΝΙΙ ГОСУДАРСТВЕННОГО ТЕСТИРОВАНИЯ ПО РУССКОМУ ЯЗЫКУ των Ομοσπονδιακών κρατικών ιδρυμάτων ανώτατης εκπαίδευσης της Ρωσικής Ομοσπονδίας, «Κρατικού Ινστιτούτου της ρωσικής γλώσσας Α.Σ.Πούσκιν», «Κρατικού Πανεπιστημίου της Μόσχας Μ.Β.Λομονόσοβ», «Ρωσικού Πανεπιστημίου της Φιλίας των Λαών», «Κρατικού Πανεπιστημίου της Αγίας Πετρούπολης», «Κρατικού Πανεπιστημίου της Τιουμέν» επιπέδου C2/ТРКИ-4 (ЧЕТВЕРТЫЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ)	ΣΕΡΤΙΦΙΚΑΤ Ο ΠΡΟΧΟΖΔΕΝΙΙ ГОСУДАРСТВЕННОГО ТЕСТИРОВАНИЯ ПО РУССКОМУ ЯЗЫКУ των Ομοσπονδιακών κρατικών ιδρυμάτων ανώτατης εκπαίδευσης της Ρωσικής Ομοσπονδίας, «Κρατικού Ινστιτούτου της ρωσικής γλώσσας Α.Σ.Πούσκιν», «Κρατικού Πανεπιστημίου της Μόσχας Μ.Β.Λομονόσοβ», «Ρωσικού Πανεπιστημίου της Φιλίας των Λαών», «Κρατικού Πανεπιστημίου της Αγίας Πετρούπολης», «Κρατικού Πανεπιστημίου της Τιουμέν» επιπέδου C1/ТРКИ-3 (ТРЕТИЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ)	ΣΕΡΤΙΦΙΚΑΤ Ο ΠΡΟΧΟΖΔΕΝΙΙ ГОСУДАРСТВЕННОГО ТЕСТИРОВАНИЯ ПО РУССКОМУ ЯЗЫКУ των Ομοσπονδιακών κρατικών ιδρυμάτων ανώτατης εκπαίδευσης της Ρωσικής Ομοσπονδίας, «Κρατικού Ινστιτούτου της ρωσικής γλώσσας Α.Σ.Πούσκιν», «Κρατικού Πανεπιστημίου της Μόσχας Μ.Β. Λομονόσοβ», «Ρωσικού Πανεπιστημίου της Φιλίας των Λαών», «Κρατικού Πανεπιστημίου της Αγίας Πετρούπολης», «Κρατικού Πανεπιστημίου της Τιουμέν» επιπέδου B2/ТРКИ-2 (ВТОРОЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ)	ΣΕΡΤΙΦΙΚΑΤ Ο ΠΡΟΧΟΖΔΕΝΙΙ ГОСУДАРСТВЕННОГО ТЕСТИРОВАНИЯ ПО РУССКОМУ ЯЗЫКУ των Ομοσπονδιακών κρατικών ιδρυμάτων ανώτατης εκπαίδευσης της Ρωσικής Ομοσπονδίας, «Κρατικού Ινστιτούτου της ρωσικής γλώσσας Α.Σ.Πούσκιν», «Κρατικού Πανεπιστημίου της Μόσχας Μ.Β.Λομονόσοβ», «Ρωσικού Πανεπιστημίου της Φιλίας των Λαών», «Κρατικού Πανεπιστημίου της Αγίας Πετρούπολης», «Κρατικού Πανεπιστημίου της Τιουμέν» επιπέδου B1/ТРКИ-1 (ПЕРВЫЙ СЕРТИФИКАЦИОННЫЙ УРОВЕНЬ)

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	РУССКИЙ ЯЗЫК - ДИПЛОМ ПУШКИН (ΙΝΣΤΙΤΟΥΤΟ ΠΟΥΣΚΙΝ ΑΘΗΝΩΝ)	РУССКИЙ ЯЗЫК – ПОСТПОРОГОВЫЙ УРОВЕНЬ (ΙΝΣΤΙΤΟΥΤΟ ΠΟΥΣΚΙΝ ΑΘΗΝΩΝ)	РУССКИЙ ЯЗЫК – ПОРОГОВЫЙ УРОВЕНЬ (ΙΝΣΤΙΤΟΥΤΟ ΠΟΥΣΚΙΝ ΑΘΗΝΩΝ)	РУССКИЙ ЯЗЫК – ЭЛЕМЕНТАРНЫЙ УРОВЕНЬ (ΙΝΣΤΙΤΟΥΤΟ ΠΟΥΣΚΙΝ ΑΘΗΝΩΝ)
	Κρατικό πιστοποιητικό γλωσσομάθειας επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	Κρατικό πιστοποιητικό γλωσσομάθειας επιπέδου Β1 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003
	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΑΡΑΒΙΚΑ	Certificate of the Arabic Language Proficient Level – C2 του Πανεπιστημίου «An-Najah National University της Nablus»	Certificate of the Arabic Language Advanced Level – C1 του Πανεπιστημίου «An-Najah National University της Nablus»	Certificate of the Arabic Language Experienced Level – B2 του Πανεπιστημίου «An-Najah National University της Nablus»	Certificate of the Arabic Language Intermediate Level – B1 του Πανεπιστημίου «An-Najah National University της Nablus»
	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΑΛΒΑΝΙΚΑ	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΒΟΥΛΓΑΡΙΚΑ	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΡΟΥΜΑΝΙΚΑ	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΣΕΡΒΙΚΑ	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
ΤΟΥΡΚΙΚΑ	Πιστοποιητικό αντίστοιχου επιπέδου (C2, C1, B2, B1) που εκδίδεται και χορηγείται από το Ίδρυμα Μελετών Χερσονήσου του Αίμου (ΙΜΧΑ) μετά από εξετάσεις (άρθρο 248 ν. 4610/2019) και με την προϋπόθεση ότι τα Πιστοποιητικά έχουν εκδοθεί μετά την 7-5-2019, ημερομηνία δημοσίευσης του ανωτέρω νόμου.			
	Κρατικό πιστοποιητικό γλωσσομάθειας	Κρατικό Πιστοποιητικό Γλωσσομάθειας	Κρατικό Πιστοποιητικό Γλωσσομάθειας	Κρατικό πιστοποιητικό γλωσσομάθειας επιπέδου Β1 του

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΛΩΣΣΟΜΑΘΕΙΑΣ				
ΞΕΝΗ ΓΛΩΣΣΑ	**ΕΠΙΠΕΔΟ C2 (ΑΡΙΣΤΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ C1 (ΠΟΛΥ ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B2 (ΚΑΛΗ ΓΝΩΣΗ)**	**ΕΠΙΠΕΔΟ B1 (ΜΕΤΡΙΑ ΓΝΩΣΗ)**
	επιπέδου Γ2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	επιπέδου Γ1 του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	επιπέδου Β2 του ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003	ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003

- **Η άριστη γνώση οποιασδήποτε ξένης γλώσσας** διαπιστώνεται με το οικείο κατά περίπτωση γλώσσας:

  (i) πτυχίο ή δίπλωμα Αγγλικής Γλώσσας και Φιλολογίας ή Γαλλικής Γλώσσας και Φιλολογίας ή Γερμανικής Γλώσσας και Φιλολογίας ή Ιταλικής Γλώσσας και Φιλολογίας ή Ιταλικής και Ισπανικής Γλώσσας και Φιλολογίας ή Ισπανικής Γλώσσας και Φιλολογίας ή Ρωσικής ή Τουρκικής ή Βουλγαρικής ή Ρουμανικής Γλώσσας, Φιλολογίας και Πολιτισμού Παρευξείνιων Χωρών ή Ρωσικής Γλώσσας και Φιλολογίας και Σλαβικών Σπουδών εισαγωγική κατεύθυνση Ρωσικής Γλώσσας και Φιλολογίας ή Τουρκικών Σπουδών και Σύγχρονων Ασιατικών Σπουδών ή Ισπανικής Γλώσσας και Πολιτισμού ή Ξένων Γλωσσών, Μετάφρασης και Διερμηνείας ΑΕΙ της ημεδαπής ή ακαδημαϊκά ισοδύναμος ή ισότιμος τίτλος σχολών της ημεδαπής ή αλλοδαπής, αντίστοιχης ειδικότητας.

  (ii) Πτυχίο, προπτυχιακό ή μεταπτυχιακό δίπλωμα ή διδακτορικό δίπλωμα οποιουδήποτε αναγνωρισμένου ιδρύματος τριτοβάθμιας εκπαίδευσης της αλλοδαπής, συνοδευόμενο από σχετική βεβαίωση του ιδρύματος για τη γλώσσα στην οποία πραγματοποιήθηκαν οι σπουδές, εφόσον αυτή διαφοροποείται από την επίσημη γλώσσα της οικείας χώρας.

  (iii) Μεταπτυχιακό δίπλωμα στο πλαίσιο συνεργασίας εκπαιδευτικού ιδρύματος τριτοβάθμιας εκπαίδευσης της ημεδαπής με αναγνωρισμένο ομοταγές της αλλοδαπής ή με μεταπτυχιακό δίπλωμα της ημεδαπής, εφόσον η γλώσσα διδασκαλίας, των εξετάσεων, της συγγραφής και της παρουσίασης της μεταπτυχιακής εργασίας είναι άλλη πλην της ελληνικής κατά τα οριζόμενα στις οικείες διατάξεις, συνοδευόμενο από σχετική βεβαίωση του ιδρύματος για τη γλώσσα στην οποία πραγματοποιήθηκαν οι σπουδές.

- **Η πολύ καλή γνώση οποιασδήποτε ξένης γλώσσας αποδεικνύεται με:**

  (i) απολυτήριο τίτλο ή πτυχίο αναγνωρισμένου ξένου σχολείου δευτεροβάθμιας εκπαίδευσης της ημεδαπής κατά την παρ. 8 του άρθρου 35 του ν. 4186/2013 (Α΄ 193), όπως ισχύει, εφόσον τα μαθήματα διεξάγονται αποκλειστικά σε άλλη γλώσσα πλην της ελληνικής, συνοδευόμενο από σχετική βεβαίωση του σχολείου για τη γλώσσα στην οποία πραγματοποιήθηκαν τα μαθήματα,

  (ii) απολυτήριο τίτλο ή πτυχίο σχολικής μονάδας της αλλοδαπής δευτεροβάθμιας ή μεταδευτεροβάθμιας εκπαίδευσης, ισότιμο των ελληνικών σχολείων Δευτεροβάθμιας Εκπαίδευσης, εφόσον έχει αποκτηθεί μετά από κανονική φοίτηση τουλάχιστον έξι ετών στην αλλοδαπή, συνοδευόμενο από:

  α) βεβαίωση ισοτιμίας για το επίπεδο της εκπαιδευτικής βαθμίδας στην οποία ανήκει, που χορηγείται από τον ΟΕΕΚ ή ΕΟΠΠ ή ΕΟΠΠΕΠ ή από την αρμόδια Διεύθυνση του Υπουργείου Παιδείας έπειτα από την έκδοση της αντίστοιχης ατομικής διοικητικής πράξης ισοτιμίας ή/και

β) βεβαίωση της σχολικής μονάδας για τη γλώσσα στην οποία πραγματοποιήθηκαν οι σπουδές, εφόσον αυτή διαφοροποιείται από την επίσημη γλώσσα της οικείας χώρας.

- Η άριστη (Γ2 ή C2), πολύ καλή (Γ1 ή C1), καλή (Β2 ή B2) και μέτρια (Β1ή B1) γνώση οποιασδήποτε ξένης γλώσσας διαπιστώνεται με αντίστοιχου επιπέδου **Κρατικό Πιστοποιητικό Γλωσσομάθειας** του ν. 2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003.

Γενικές επισημάνσεις:

- Τίτλοι σπουδών γνώσης ξένης γλώσσας υπερκείμενου επιπέδου αποδεικνύουν και τη γνώση κατώτερου (ζητούμενου) επιπέδου της ξένης γλώσσας.

- Η άδεια επάρκειας διδασκαλίας ξένης γλώσσας, δεν αποδεικνύει την γνώση ξένης γλώσσας. Οι υποψήφιοι κάτοχοι της σχετικής άδειας πρέπει να αποδείξουν τη γνώση της ξένης γλώσσας με έναν από τους οριζόμενους τρόπους απόδειξης αυτής που περιλαμβάνονται στο παρόν Παράρτημα.

- Όλοι οι τίτλοι σπουδών ξένης γλώσσας πρέπει να συνοδεύονται από επίσημη μετάφρασή τους στην ελληνική γλώσσα.

ΠΑΡΑΡΤΗΜΑ Α3

ANNEX 1

Horizon Europe (HORIZON)

Description of the action (DoA)

Part B

Version 0.5
30 April 2024

Contents

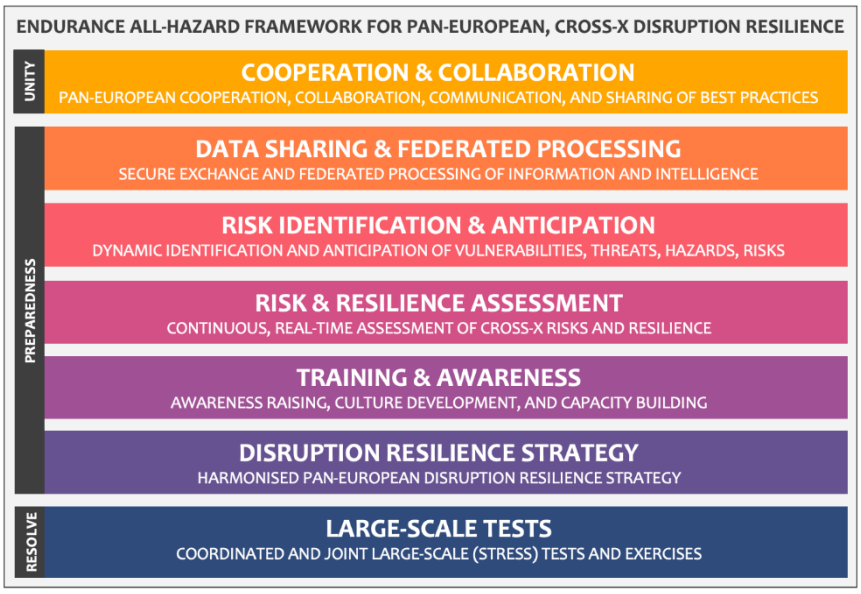
History of Changes

HISTORY OF CHANGES		
Part B		
Date	**Page/Section**	**Nature of change and reason / justification of change proposed**
04/04/2024	Page 8, 9, 10, 12, 14, 15, 16, 17, 18, 19, 20, 21, 23, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 43, 45, 46, 49, 50, 52, 53, 54, 57, 58, 62	Updated WP, task and deliverable numbers according to latest Gantt chart
	Page 61	Updated Security Officer
10/04/2024	Page 62 & 63	Updated relevant expertise of SAB members
	Page 56, 57, 58, 59, 60, 61, 63	Deleted the instructions boxes
	Section 3.1.1	Added chapter 3.1.1.Overall Structure of the Work Plan and updated the task, WP and deliverables numbers to the latest WP structure as discussed with the Project Officer
17.04.2024	Page 2&6	Removed pages 2 & 6, as page 2 has instructions and page 6 is empty
	Section 3.2.4	Section 3.2.4 »Affiliated Entities« added, with information about Eviden DE
	Section 3.2.5	Section 3.2.5 »Role and budget of Associated Partners« added
	Section 3.1.2	In Section 3.1.2 kept only Subcontracting costs table
	Section 6	»Information about security practitioners« chapter moved to the end of the document
	Section 5.1	In the deliverables table, kept only the deliverables present in the Security Evaluation Summary Report. In parentheses, kept the former deliverable numbers (as in the Proposal).
	Secton 5.2.1	Deleted sub-sections, kept only the sentence related to the project not producing classified information.
	Section 5.2.3	Project Security Board replaced with Security Advisory Board
	Section 5.4	Confirmation for implementing the measures forseen in the Tackling R&I foreign interference added.
22.04.2024	Section 1.1.1 , 1.2.1, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.8, 2.1.1, 2.1.3, 2.2.2, 2.2.3, 3.1.1, 3.2.3, 4.1, 4.2, 5.4	As WP 11 for IMPACT is comprising both phases (1&2), deliverables and task numbers are updated accordingly.
	Section 3.1.1	As WP 11 for IMPACT is comprising both phases (1&2), the figure with the WPs & the Gantt chart are updated accordingly.
30.04.2024	Section 3.2.4	Cost and granted amount for Eviden Germany are updated according to PM rate.
	Section 5, 5.1, 5.3.1, 5.4	Updated according to feedback from Project Officer
	Sections Security Aspects Letter, Security Classification Guide, Project Security Officer	Removed as not manadatory (feedback from the Project Officer)

1. Excellence

1.1. Ambition

1.1.1. Motivation and Objectives



Amidst an increasingly interconnected and complex world, the provision of essential services remains crucial for the well-being of European citizens and the smooth functioning of the internal market. Yet, the ever-evolving landscape of risks, ranging from cyber threats, physical attacks, and human errors to natural disasters, demands a proactive and collaborative, pan-European approach to ensuring disruption resilience. Therefore, ENDURANCE is driven by the critical need to **fortify Europe's essential services** against potential disruptions, **transcending the sole focus on the underlaying critical assets.**

Recognizing the significance of the Critical Entity Resilience (CER) and NIS2 Directives in setting the groundwork for resilience and, in parallel, the current silo approach to the Critical Infrastructure (CI) resilience and business continuity of essential services they provide, we will assist the CI authorities across Europe in **fully grasping and harmoniously implementing both directives**. By comprehensively understanding and preparing for the demands of these legislative measures (and their national implementations), we aim to **empower the CI authorities** and, consequently, the CI operators and other relevant stakeholders with the know-how, methodologies, services, and strategies needed to navigate the complexities of disruption resilience effectively.

At the heart of the project lies the **ethos of collaboration and cooperation** at all levels. We are committed to fostering active engagement of CI authorities, operators, and other relevant stakeholders as well as the innovators, scientists, and consultants working in the area – across the geographical and sectoral boundaries. Through inclusive and diverse participation, we envision a united front against disruptions to essential services, thus ensuring **comprehensive preparedness and effective response capabilities against disruptions caused by any threat or hazard**.

Our ambitions extend beyond theoretical frameworks. While conducting in-depth analyses of the interdependencies of various essential services, and the pertaining threats, hazards, and risks is fundamental, we take a proactive stance by developing comprehensive **methodologies, interoperable technologies, and pragmatic strategies** to increase their resilience. Our dedication does not stop there; we will rigorously **(stress) test these solutions** in a joint, synchronised, and cross-sector/-border manner to ensure their real-world effectiveness and scalability. Moreover, to bolster Europe's preparedness, we will provide **comprehensive and immersive training materials and services**, empowering the human chain with the knowledge and skills to address disruptions confidently and effectively.

In an ever-changing landscape of challenges, ENDURANCE stands as a testament to the power of collaboration, proactive disruption resilience, and a unified European response to safeguard essential services, the well-being of European citizens, and prosperity and sovereignty of the European economy. By fostering cooperation, sharing knowledge, and harmoniously implementing robust strategies and technologies, we aspire to **strengthen Europe's resilience and secure a future where disruptions are met with preparedness, resolve, and unity**.

OUR MISSION: As illustrated above, we undertake targeted activities to: **(i) Enhance strategic cooperation and collaboration** among the European CI stakeholders at all levels (bringing together 100+ relevant practitioners and experts across Europe). **(ii) Develop datasets, registries, methodologies, technologies, and services** (at TRL6-7) for secure sharing and federated processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness. **(iii) Provide harmonised and pragmatic strategy** for the continuity of the interconnected essential services (adopted by 20+ relevant European sectorial and national CI authorities).

Objective #1 – UNITY: Encourage, enhance, and support the all-level, pan-European **strategic cooperation, operational collaboration, and continuous communication**, enabling exchange of experience and best practices.

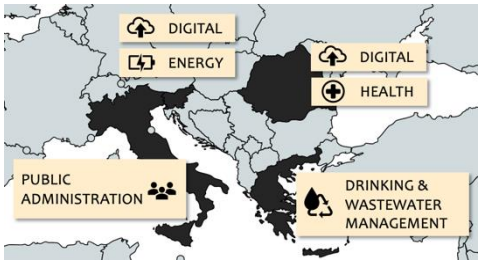
Related WPs: **WP1&WP2** **Key Results and KPIs**: See Section 1.1.2.1 (**means for cooperation**)

We will organise **12 national and 3 European workshops** with competent authorities from different EU Member States (MSs), CI operators, and other relevant CI stakeholders to establish a framework for understanding the current functioning of the European CI and provide cooperation mechanisms at different levels: Local, regional, national, cross-border; Within and across sectors; Between public and private entities; With governments and policy makers.

These workshops will serve as means for strengthening relationships among the CI stakeholders, for exchanging knowledge, experience, and best practices among them, and for gathering inputs for the development and co-creation of the ENDURANCE results. Enhanced strategic cooperation, active collaboration, and continuous communication among the CI stakeholders will enable faster identification of potential challenges and gaps, and faster identification of effective solutions and coordinated actions for better joint resilience against disruptions. The workshops will be gradually transformed into a **Working Group on Disruption Resilience** (**WGDR**, with 100+ members by the end of the project) that will independently continue activities after the project end.

We will continuously explore existing initiatives, networks, and working groups (e.g., the Critical Entities Resilience Group (CERG), NIS2 Cooperation Group, or relevant working groups established in EU-funded projects, e.g., the SUNRISE Working Group on pandemic resilience) and **seek liaisons** with them when establishing the WGDR. The WGDR will thereby provide a dynamic environment for **active engagement of various CI stakeholders at all levels and across various sites, organisations, sectors, and borders**. With the support of the practitioners and experts participating in the WGDR, we will gather, merge, and share the know-how and experience in ensuring resilience of essential services, and, with that, **harmonise the understanding and support the implementation of the resilience-focused European, national, and sectorial legislation** (e.g., CER and NIS2 Directives).

The consortium includes **7 competent authorities** (national, regional, sectorial) and **6 public and private CI operators from 6 different sectors** (digital, energy, health, public administration, drinking water, wastewater) from **4 different EU MSs** (Slovenia, Romania, Italy, Greece) as illustrated on the right. Their participation in project workshops and the WGDR will be **extended to other organisations outside the consortium** representing other sectors and countries to ensure that our results reflect the needs of different stakeholders across the EU, to promote our results to a wide audience, and to facilitate the spirit of collaboration and unity beyond the project end.

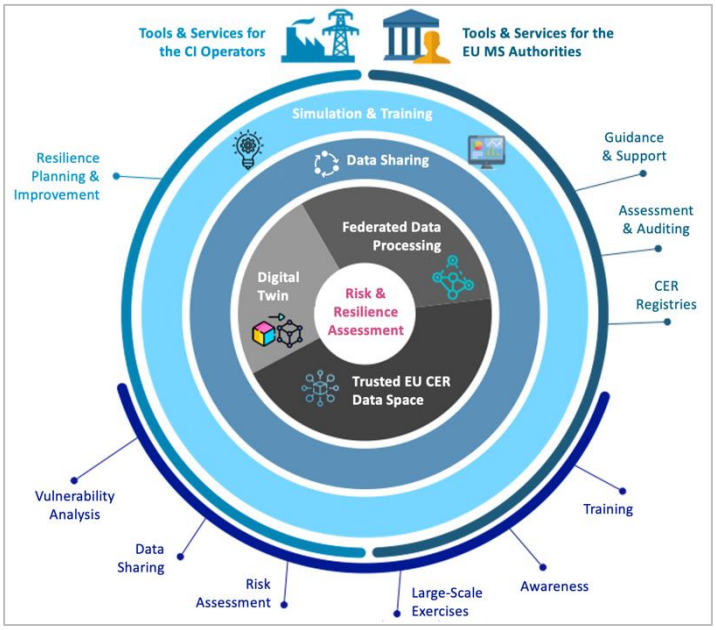


Objective #2 – PREPAREDNESS WITH SERVICES: Establish a **trusted data space** for CER-relevant data and deliver user-friendly and interoperable services for **(1) secure exchange and federated processing** of such data, **(2) essential-service-oriented digital twins**, **(3)** continuous **identification and assessment of risks and resilience**, and **(4) human-centric simulation and interactive training**, empowering a broader community of CI stakeholders.

Related WPs: **WP3-WP8** **Key Results and KPIs**: See Sections 1.1.2.2-1.1.2.6 (**enablers and services**)

The goal of ENDURANCE is to define and set the basis for an **EU-wide ecosystem of data, models, methods, tools, and services to support the competent EU MS authorities and CI operators** in evaluating, understanding, and proactively ensuring resilience of essential services against potential cyber and physical threats and risks, including natural hazards. The focus of ENDURANCE is on public or private Critical Entities (CE), as defined by the CER Directive, that are providing essential services, which are crucial for the functioning of the vital societal functions, economic activities, public health and safety, and the environment. Our aim is to **enhance their resilience**, intended as "*the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from an incident*" that have the potential to (significantly) disrupt the provision of essential services.

In accordance with the CER Directive, EU MS and their competent authorities (responsible for resilience on national level and/or for overseeing operators) play a fundamental role in the overall risk assessment process. These authorities are pivotal in evaluating the nature and scope of risks, encompassing cyber and physical (incl. natural) elements. This involves **(i)** the **identification and analysis of potential vulnerabilities, threats, and hazards** that may escalate to (severe) incidents and (significant) essential service disruptions, and **(ii)** the **assessment of the potential (negative) impact or loss** resulting from such incidents and disruptions.



To this end, as shown on the right, ENDURANCE will deliver **tools and services** **(i)** for **CI authorities** (listed on the right side) **(ii)** for **CI operators**, (on the left) and **(ii)** those **common to both** (on the bottom). They will be developed with a multi-tiered set of features, building an integrated cross-entity/-sector/-country (**cross-X**) **intelligence framework that transcends individual entities, sectors, and boundaries**.

The tools will be based on **results of Horizon Europe projects** (at TRL4) and matured to reach **TRL6-7**

The baseline for the development of the tools and services will be a **Trusted EU CER Data Space**, a registry jointly established, maintained, and used by the CI authorities and operators, which will include **harmoniously defined and identified** essential services, critical entities, their interdependencies, and associated risks and potential impacts.

Objective #3 – PREPAREDNESS WITH STRATEGY: Align and improve current practices, policies, strategies, and business continuity plans by generating a harmonised **pan-European strategy for disruption resilience**.

Related WPs: **WP1&WP2** **Key Results and KPIs**: See Section 1.1.2.1 (**strategy**)

Insights into the existing practices, policies, technologies, gaps, and challenges provided by **(i)** the CI stakeholders during the workshops [**WP1&WP2**], **(ii)** the desk research and innovation activities [**WP3-WP8**], and **(iii)** the results of the large-scale exercises [**WP9&WP10**] (see Objective #4) will serve as a baseline for the development of a comprehensive, harmonised, evidence-based, pragmatic, European **Strategy for Disruption Resilience** that will include **(i)** common interpretations of the **CER definitions**, **(ii)** harmonised methodologies for all-hazard, cross-x **risk and resilience assessment**, **(iii)** guidelines for an effective, joint, cross-x **disruption response**, and **(iv)** new models for coordinated **crisis communication**, aligned with the significant shifts in our society caused by pandemic, political conflicts, economic crisis, and natural disasters.

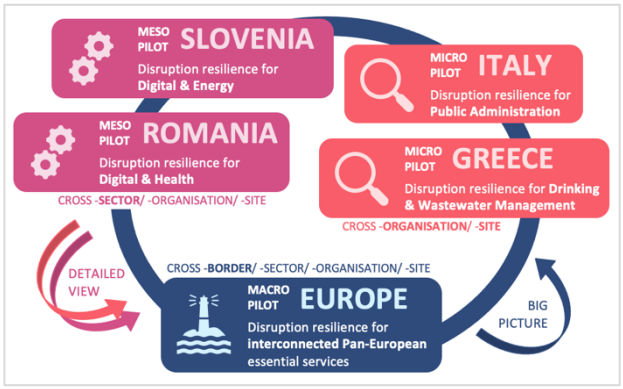
Objective #4 – RESOLVE THROUGH TEST: Design and coordinate **large-scale and cross-x exercises** with CI authorities and operators to **stress test** their preparedness and ensure that our results are effective and pragmatic.

Related WPs: **WP9&WP10** **Key Results and KPIs**: See Sections 1.1.2.7 and 1.2.3 (**stress tests** and **pilots**)

Based on the know-how obtained through the international collaboration of various experts and practitioners, we will design and implement **scenarios and plans for coordinated, cross-x, large-scale (stress) tests** to ensure that the developed methodologies, strategies, tools, and services for disruption preparedness are effective, efficient, and pragmatic. These will be aligned with the EC's "CI Blueprint" and will rely on various simulation and training tools.

The designed tests will serve as a baseline for the large-scale exercises run in **5 strategic and operational pilots** involving **4 EU MS** and representatives of **6 critical sectors** (as defined by the CER Directive). In these pilots, all ENDURANCE results will be tested, demonstrated, and **validated in relevant/operational environments** with the end users participating in the project, thereby facilitating more disruption resilient essential services in Europe:

- **MACRO Pilot EUROPE**: Involving all CI authorities and operators, we will capture and tackle challenges on a **cross-border**, **strategic** scale. In this pilot, we will primarily focus on the evaluation of the **Strategy** and **Risk & Resilience Assessment Service** to **directly support the Cis in the implementation of the CER Directive**.
- **MESO Pilots SLOVENIA and ROMANIA**: We will identify, analyse, and address the **cross-sector** challenges on a local, regional, and national level in Slovenia and Romania within and across the Digital-Energy and Digital-Health sectors, respectively. In these two pilots, we will primarily focus on the evaluation of the **Digital Twin** to demonstrate and closely analyse the cross-sector interdependencies.
- **MICRO Pilots ITALY and GREECE**: We will capture the specificities of the individual countries, regions, and sectors, focusing on the **cross-entity, cross-site, and cross-region** aspects in Italy and Greece in the Public administration and the (Drinking and Waste) Water Management sectors, respectively. In these two pilots, we will primarily focus on the evaluation of the **Simulation & Training Service** to evaluate usability aspects.



Objective #5 – PROMOTE: **Promote the ENDURANCE mission, activities, and results** to the relevant CI stakeholders across Europe and **generate great positive, direct, tangible, and immediate impacts**.

Related WPs: **WP11** **Key Results and KPIs**: See Section 2.2 (**impact generation**)

Throughout the project, we will execute tailored **communication, dissemination, standardisation, exploitation, and policy making activities** targeted at specific audiences to **(i)** increase **awareness** about the relevant threats and hazards, **(ii)** spread knowledge about **new means** to prepare for their potential impacts, and thereby increase resilience of essential services, and **(iii)** facilitate cooperation opportunities among various CI stakeholders.

We will also define a framework for a **quantitative and qualitative assessment of the positive impacts** that the ENDURANCE solutions have on the **society, economy, and environment**, and continuously assess them. [**T11.5**].

The consortium includes a group of policy makers and practitioners, industry experts, engineers, researchers, and SSH experts with dedicated know-how, experience, and networks that will **(i) bring valuable feedback** from the external communities to the consortium, facilitating the tailoring of the results to the needs of a wider group of users and market, and **(ii) actively promote our results** within their networks, facilitating wider and bigger impact fast.

1.1.2. Ambition, Project Results, Maturity

1.1.2.1. Enhancing Pan-European Cooperation, Collaboration, Communication [WP1&WP2]

Challenges: Many recent events such as pandemic, wars, and ever more severe and frequent natural disaster have dramatically highlighted the importance of the **resilience** of the European (critical) infrastructure and **continuity and security** of the essential services they support. However, there is a big challenge in having the CI authorities (and CI operators) discussing and joining forces to better understand the **needs** of the operators in identifying and anticipating risks, assessing and ensuring resilience, and managing (potential) significant disruptions, and **ways** to meet them. This challenge stems from different aspects, including from the **(i) lack of suitable mechanisms and environments** for exchanging views and best practices, and for setting up strategic cooperation and operational collaboration among the CI stakeholders for joint risk assessment, training, and (stress) testing exercises, and **(ii) large diversity in terms of definitions, methodologies, procedures, best practices, and policies** across organisations, sectors, and borders, **hindering cross-x cooperation, coordination, and harmonisation in the implementation of the CER Directive**.

The Commission has set up the **Critical Entities Resilience Group (CERG)** to provide support on cross-x risks, best practices, methodologies, training, and exercises to test the resilience of Critical Entities (CEs). However, it **only includes an expert group of EU MS authorities** to discuss the provisions of the CER Directive and their direct and indirect impact, as well as all other matters related to the CI resilience. Similarly, the Commission has established the **NIS2 Cooperation Group** (**NIS2-CG**) that is composed of

representatives of the Commission, ENISA, and EU MSs. However, for a thorough understanding of the impacts of the CER and NIS2 Directives and the operational challenges of the CI operators in implementing them, a **wider discussion and synchronisation is needed** that also includes the CI operators and other relevant CI stakeholders (e.g., technology providers, researchers).

Currently, the EU MS authorities (national, regional, sectoral) **use different practices, guidelines, and policies** for the management of resilience of the essential services they supervise and **impose different requirements** on the CI operators they oversee to assess and ensure resilience. They also may have **different interpretations** of the different terms and provisions and are at **different maturity levels** in their implementation into the national legislation and/or at operational level. This diversity in definitions, practices, guidelines, and policies among the authorities results in a **lack of harmonization and standardization in the management of resilience** for the connected cross-x essential services. The consequence is a fragmented landscape where CI operators face varying requirements and expectations depending on the jurisdiction they fall under. This lack of uniformity can lead to challenges like **(i) inconsistencies** where the CI operators may struggle to comply with disparate sets of requirements and regulations, making it difficult to establish consistent resilience practices, **(ii) complexity and administrative burdens** that stem from the need to navigate and adhere to different guidelines, potentially diverting resources away from the actual enhancement of resilience, **(iii) inefficiencies** resulting in duplicated efforts as CI operators address similar resilience goals using different methodologies, tools, or standards due to the absence of a unified approach, **(iv) vulnerabilities** created by inconsistencies in resilience requirements, leaving certain critical sectors or services more vulnerable due to variations in preparedness and response measures, and **(v) interoperability issues** caused by differences in resilience approaches, impeding effective collaboration and response efforts in cases of cross-border or cross-sector incidents.

Ambition: Addressing this situation requires a concerted effort to harmonize definitions, methodologies, practices, guidelines, and policies, and thereby create a more cohesive and collaborative environment for managing resilience across essential services within the EU. To this end, we will **(i) establish effective mechanisms and environments for strategic cooperation, operational collaboration, and effective communication** among the EU MS authorities, Ci operators, and all other relevant stakeholders (participating or enabling the essential services' supply chains), and **(ii) jointly design, thoroughly test, and continuously improve a pan-European harmonised Strategy for Disruption Resilience**, with which we will directly support the competent EU MS authorities and CI operators in the implementation of / compliance with the CER and NIS2 Directives (and other relevant mechanisms).

Realisation: To ensure that ENDURANCE adds maximum value, we will first explore and understand the strategic environment and the operational specifics of individual elements of the European CI, their interdependencies, as well as their individual and common challenges. To this end, we will establish a platform for collaboration among the relevant CI stakeholders in the form of a **Working Group on Disruption Resilience**, by **(i)** utilising existing efforts and **seeking liaisons with groups** like CERG, NIS2-CG, and other working groups and clusters operating at the EU-funded project level (e.g. the European Cluster for Securing Cis – ECSCI), and **(ii)** leveraging existing and future networks to **engage the right experts** on different dimensions of the CI and resilience. A strong focus will be put on ensuring active participation of **competent authorities across the entire EU and all CER-defined critical sectors**.

Discussions with the CI authorities, operators, and other stakeholders will take place in a series of dedicated **local (national and/or regional) and international (European) workshops**. These will provide important opportunities to **(i) identify the perspective and/or expertise missing** in the Working Group to continuously enrich it, **(ii) discuss and harmonise** established definitions (incl. on what constitutes a disruptive event), methodologies, practices, and policies to ensure effective and coordinated efforts in managing resilience across the EU, **(iii) identify, discuss, and solve strategic challenges** related to the understanding, assessing, and managing resilience, and **(iv) jointly establish and validate the European Strategy for Disruption Resilience**. The Strategy will comprise a set of methodologies, procedures, protocols, and models for **(i)** all-hazard, cross-x **risk and resilience assessment**, **(ii)** an effective, joint, cross-x **disruption response**, and **(iii)** coordinated **crisis communication**.

To deal with future (large-scale and cross-x) disruptions to essential services more effectively, it is necessary to consider relevant social factors since legal-technical approaches are sometimes not a realistic reflection of the needs of society. To this end, we will make a **significant SSH contribution** in our interaction with the CI authorities and operators by **engaging the SSH experts** included in the consortium in the project workshops.

Result	Type	KPI & Target Value	Target TRL

A Pan-European Working Group on Disruption Resilience	Network	**>50** members by end of Year 1 **>80** members by end of Year 2 **>100** members by end of Year 3	N/A
Local and Pan-European workshops on CI resilience	Event	**>15** events in total **>20** participants at each event on average	N/A
Strategy for Disruption Resilience	Guideline	**>30** representatives of competent EU MS authorities and **>60** representatives of CI operators from all critical sectors reviewing it	N/A

1.1.2.2. Trusted EU CER Data Space [WP5&WP6]

Challenges: Enabling secure data exchange to support cross-operator, cross-sector, and cross-border risk assessment and resilience analysis in the EU CI presents a set of complex challenges. The diverse nature of CI poses **interoperability challenges** as each sector (or each operator) may have unique data formats, protocols, and security standards. The need for seamless cross-operator collaboration introduces concerns about **data privacy, confidentiality, and compliance** with varying regulations across EU MS. Furthermore, achieving a balance between sharing critical information for comprehensive risk assessments and protecting sensitive details from potential cyber threats requires **robust cybersecurity measures and a trusted data ecosystem**. Furthermore, **clear ownership rights and data-sharing agreements** are crucial to establish trust and facilitate collaboration among stakeholders. Building trust among different operators and sectors for sharing sensitive data is a significant hurdle, as entities may be reluctant to disclose vulnerabilities or incidents. Additionally, the dynamic and evolving nature of cyber threats **demands a constant reassessment of risk and resilience strategies**. Addressing these challenges **necessitates coordinated efforts in harmonising data formats, establishing clear data governance frameworks, fostering a culture of information sharing, and introducing advanced cybersecurity technologies** to ensure the secure exchange of critical data across borders and sectors within the European Union.

Ambition: ENDURANCE will go beyond secure data exchange by **enabling the creation of a trusted, sustainable, and accountable Data Ecosystem**, encouraging the creation and management of diverse data spaces for sharing of relevant data supporting cross-x risk assessment and resilience analysis, ensuring adherence to European values and principles concerning data protection, privacy, and ethics. These data spaces serve as collaborative environments where stakeholders, including operators and authorities, can **securely deposit, share, and collaboratively generate data and intelligence** related to the CI resilience. Moreover, to operationalise the data space, we will identify critical entities in EU MS, define the interconnected essential services they provide, and **model interdependencies between these services, surpassing the sole focus on critical assets**.

Realisation: Our Trusted EU CER Data Space will be **designed on top of the reference architectures** for **Federated and Secure Data Infrastructure** (i.e., GAIA-X) and **Data Spaces** (i.e., IDSA). This is an original approach for data sharing in CI protection and resilience, which can benefit from all design principles of those reference architecture and frameworks, especially in terms of data security, sovereignty, governance, and access controls to safeguard sensitive information, leveraging on sound standardization and interoperability efforts. Standardizing data formats and structures facilitates smooth data exchange, enabling a more comprehensive understanding of risks and vulnerabilities. The data about the identified critical entities, essential services, and their interdependencies will be generated **based on the know-how from previous INFRA projects** like ATLANTIS, SUNRISE, and PRECINCT.

Result	Type	KPI & Target Value	Target TRL
CER Data Models	Specification	**>5** different CER data facets modelled. **>10** data sources harmonised, aligned, integrated.	N/A
Data Governance & Security Infrastructure for Trusted EU CER Data Spaces	Innovative Solution	**>5** data sources enabled. **>7** data consumers enabled and supported.	TRL7

1.1.2.3. Secure Exchange and Federated Processing of Sensitive Data [WP7&WP8]

Challenges: The evolving digital transformation expands and encompass CI systems as well. For example, in the energy domain, the traditional Power Plants are now more and more complemented by distributed micro-grids, RES and storage systems, while traditional consumers turn into prosumers, who gain direct access and contribute to the overall electricity mix. As a result, today's electricity systems do not only experience a significant expansion on their potential attack surface, **but also face a substantial**

rise in the likelihood of privacy violations and breaches of personal data, as energy consumption and production data can reveal personal profile information either explicitly or implicitly. On the other hand, *the race against cybercrime is lost without AI-based tools and decision support systems (DSS), which in return* **need sufficient data to become properly trained**, while coordinated cross-CI protection needs by definition **secure information exchange**.

Secure and trusted information exchange has been a research area since communication networks infancy. For example, strong encryption algorithms have been applied ensuring that information remains unreadable without the proper decryption keys, while Virtual Private Networks (VPNs) establish secure and encrypted communication channels over public networks, protecting data from potential eavesdropping or unauthorized access. In parallel, firewalls, access control mechanisms, security protocols such as HTTPS and SSH enforce strict access and ensure authorized access to data and resources. (Deep) packet filtering techniques are often utilized to inspect incoming and outgoing traffic, aiming to detect malicious network activity. Though successfully applied for years, these solutions introduce **significant overhead and they hardly scale**. A novel approach, initially applied in the PHOENIX project, introduces Blockchain/DLT technology in order to ensure trusted rather than cybersecure information exchange.

Beyond the technological issues and risks on data sharing, there is another challenge which may be even more difficult to be resolved: CI operators are in many cases **reluctant to share logs or data on cyber incidents**, which are necessary to train ML algorithms, due to the risk of information leakage. If not properly handed, ML models may reveal inappropriate details of the sensitive data, since models are known to implicitly memorize details during training and inadvertently reveal them during inference. Solutions to the problem adopt **federated ML and differential privacy**, which is considered as the "by default" standard in privacy preserving ML modelling.

Ambition: Due to the evolving networking paradigm, it is no longer realistic to focus on protecting central points or communication channels, but any network segment such be considered as non-trusted. Thus, in order to achieve properly trained AI models and coordinated CI cybersecurity, ENDURACE will offer secure exchange and federated processing of sensitive data considering innovative **Zero Trust methods**.

Realisation: We will innovate by offering cybersecurity of data communication via **Zero Trust Network Access (ZTNA)** methods, and by employing **Zero Trust FML**. To realise ZTNA, we will utilize (wherever available) existing legacy components offering SD-WAN, autoconfiguration of 5G micro-slices, traffic filtering/ optimization and (deep) Packet Inspection to extract traffic inceptives and traffic characteristics. Moreover, we plan to realize a Network Access Controller implementing the least privilege access principle. The controller will evaluate and extend solutions Kubernetes Network Policies, Istio, Kyverno, and Cilium to provide to devices only as much access as they really need, irrespective of their location (trusted/untrusted), following a need-to-know approach. Moreover, we will implement a Network Virtual Micro-segmentation component offering break up security perimeters into small zones to maintain separate access for separate parts of the network. Access to one of those Software-Defined Zones will not enable access any other zone without separate authorization.

With respect to ML, we will enable **Zero Trust FML (ZT-FML) training** without moving sensitive or classified data from their original sites, overcoming any legal constraints. To avoid revealing any classified, confidential, or personal information, we will leverage on homomorphic encryption methods to combine local ML training and update global models without decrypting the AI models at any location (trusted or untrusted) privately and securely.

Finally, we will securely store network and device configurations by following best practices and industry standard along with interoperable Blockchain/DLT solutions, while reducing the likelihood of malicious misconfigurations that exploited by attackers.

Result	Type	KPI & Target Value	Target TRL
Zero Trust Network Access (ZTNA)	Innovative Solution	**<5 sec** to construct **up to 5** network virtual micro-segmentation clusters. **<2 sec** to self-heal/re-configurate **up to 10** network segments.	TRL7
Homomorphic Encrypted ZT-FML	Innovative Solution	**>50%** time saving in data pre-processing. **>85%** global accuracy and **>90%** weighted global accuracy given a proper dataset federated from **10** sources	TRL7
Secure Network and Device Storage using Blockchain/DLT	Innovative Solution	**<10 sec** to store selected network configurations to blockchain. **<3** utilized interoperable Blockchain/DLTs.	TRL7

1.1.2.4. Digital Twins for Essential Services [WP5&WP6]

Challenges: Digital Twin (DT) solutions presents a ground-breaking approach to digital product representation, bridging the gap between fragmented data sources and the physical product instance. By merging physical structures with rich contextual information, this innovation revolutionizes product and service management. Today, the introduction of DT technologies has more a business-driven approach, being a powerful tool that enables industries to optimize their key business performance indicators (KPIs), emphasizing the strategic alignment of the DT technology with overarching business goals. **Operational costs present formidable challenge**. Striking the right balance between operational efficiency and cost reduction becomes a perpetual challenge. Businesses grapple with the need to optimize processes, streamline workflows, and enhance performance.

Ambition: Our vision is to pioneer the introduction of the DT through a **service resilience improvement-driven approach**, to enable proactive, informed, and agile decision-making of diverse critical sectors, setting a new standard for CI and essential services representation and management. The DT technology has the potential to provide a comprehensive understanding of essential services in the physical world and its digital counterpart. **Instead of focusing on the representation of critical assets**, we will use the DT to **create a virtual replica of an ecosystem of essential services**, with sufficient complexity to **include connections and dependencies between services**, used to simulate and test the resilience performance of services to all risks and cascading effects. It will be used to identify and analyse potential vulnerabilities, threats, and hazards that may cause essential service disruptions. It will assess the potential impact on service resilience from the perspective of disruption risks (negative) and improvement measures (positive) in early stages of CI development, operation, and maintenance.

Every essential service and CI generate data from three distinct threads: **(i)** data from the field, **(ii)** information from IT systems like SAP, PLM, and SLM, and **(iii)** tacit knowledge residing in service catalogues or within the minds of individuals. Our ambitious goal is to leverage our collaboration in WP1 (Working Group) to increase the volume of high-quality and CER-relevant data, and then **contextualize and integrate these diverse data threads**, weaving them into a cohesive 360-degree view. This metamorphosed data will feed into a robust metadata model, serving as the foundation for extracting valuable insights that will, in turn, enhance the CI and services resilience.

We aim to go beyond conventional technological applications; we aim to create an **ontology for all essential services components**, establishing a knowledge hub that not only enhances the resilience but also **serves as a training ground for individuals within the organization**. Through this holistic and resilience-centric DT approach, we aim to catalyse a paradigm shift in how Cis leverage data to drive informed decisions and enhance overall performance.

Realisation: To achieve our goals, we will leverage the existing expertise, solutions, and methodologies mainly within Eviden (EVI-RO/-DE). Our cornerstone technology is the Eviden/Atos Digital Twin platform, a robust system capable of generating a comprehensive 360-degree view of assets or processes. This platform is not a theoretical concept but has been **tested and proven in real-world scenarios**. One pivotal component is the Data Thread Contextualizer, a patented technology recognized by the European Union for its prowess in contextualizing data. This innovative tool allows us to seamlessly integrate and make sense of data coming from diverse sources.

This DT platform has already demonstrated its efficacy in the Energy industry. Through practical implementations, tangible results have been achieved, increasing asset availability by 2% and reducing the cost of operation by 10%. These successes serve as a testament to the platform's practicality and effectiveness in optimizing key business performance indicators. Building upon these accomplishments, our roadmap involves **refining and enhancing the existing platform**. We will integrate lessons learned from successful Energy industry implementations, incorporating feedback from real-world scenarios. This iterative approach ensures that our DT methodology evolves, becoming even more finely tuned to the nuances of diverse industries.

Result	Type	KPI & Target Value	Target TRL
Essential Service Models	Innovative Solution	**3** service models (digital-energy-health), including **(i)** risk model and **(ii)** resilience models. *For the MESO pilots.*	TRL6-7
Cross-X Dependencies Models	Innovative Solution	Design the connections, cross-x dependencies, and cascading effects between all 3 service models.	TRL6-7
Cross-X Risk Prediction Algorithm	Innovative Solution	Prediction algorithm to identify **(i)** potential risks within and across sectors, and **(ii)** resilience gaps within and across sectors.	TRL6-7
Stress-Test Designs	Innovative Solution	**10+** designs for stress tests covering all-hazards (for all 3 critical service models designed.	TRL6-7

1.1.2.5. Continuous Risk and Resilience Assessment [WP7&WP8]

Challenges: The state of risk and resilience assessment (within Cis as well as generally in the world) is currently dominated by qualitative methodologies, which often utilize risk matrices and expert judgment to categorize risks into various levels of severity and likelihood. While this approach has its merits in flexibility and simplicity, it lacks the precision and objectiveness that quantitative methods, like Value at Risk (VaR), can offer. This modern approach to risk assessment, which quantifies the actual expected losses in the worst-case scenarios, is the key enabler to effective risk control. Current market solutions range from standalone software platforms to integrated service offerings, with different degrees of sophistication and scalability. There is a push towards incorporating advanced technologies such as artificial intelligence and machine learning for predictive analytics, yet the implementation is still emergent and often siloed.

Most existing risk assessment frameworks **lack a robust, financial quantification of risks**, which leads to challenges in prioritizing resource allocation and mitigation efforts. There is a need for cross-sectoral risk assessment methodologies that can capture the interplay between digital infrastructure and energy service delivery, while seamlessly enabling evaluation and comparation of risks across different essential services (cross-X) with varying threat profiles and dependencies. Moreover, the dynamic nature of threats, especially in cyber domains, **necessitates real-time monitoring and assessment**, which current tools are not fully equipped to handle. The ability to perform continuous risk assessment, adapting decisions to new data and evolving threat landscapes, is underdeveloped, leaving gaps in resilience strategies. Platforms like CIRAS from ENISA provide valuable incident reporting and information sharing capabilities, yet **their integration with real-time risk assessment is limited**. Such integration is needed, as it enables learning and effective decision-making to increase the resilience, while reducing the effectiveness of this until not implemented. These challenges highlight **the need for a holistic, quantitative, and integrated approach to risk and resilience assessment** that can operate across essential service domains in real-time, leveraging and enhancing existing data sharing initiatives.

Ambition: Our ambition is to innovate beyond the traditional qualitative methods, by developing a **unified quantitative methodology**; upgrading real-time assessment technologies for **real-time monitoring and continuous risk evaluation**, which are seamlessly integrated with incident management, thereby enabling the cross-sectoral data analysis and **collaborative risk management**.

Realisation: We will achieve our ambitions by elevating the **proprietary "Silver Bullet Risk" (SBR) platform**, infusing it with advanced quantitative risk assessment know-how that we possess and will enhance during the project. We will integrate separated risk and incident management capabilities into a singular path towards seamless, continuous monitoring, which then enables robust decision-making processes. Our upgrades to existing solutions will empower the stakeholders with actionable intelligence for prompt and effective responses. Our approach is drawing from our extensive experience in quantitative risk modelling. We ensure that our upgrades reflect the latest sector-specific data and stakeholder feedback, aligning with the goal of fortifying Europe's critical infrastructures.

The SBR platform has been built for and in collaboration with various CI operators from, among others, the energy, transport, banking, and health sectors. This experience will be enriched by the experience, know-how and features built in other EU-funded INFRA projects like PRECINCT, SUNRISE, and ATLANTIS.

Result	Type	KPI & Target Value	Target TRL
Cross-border & cross-sector risk **anticipation** (predictive analytics tools that forecast risks in one country/sector that may affect organizations in another)	Innovative Solution	> 80% coverage rate of biggest known documented risks across borders and sectors	TLR7
Cross-border & cross-sector risk **monitoring** (implementation of a real-time monitoring for risks that have cross-border/sector impacts)	Innovative Solution	90% of alarms displayed through the tool when alarming value reached.	TLR7
Cross-border & cross-sector risk **alarmation** (integrated alarm system that notifies different CI operators of risks that may impact them)	Innovative Solution	90% intended alarms displayed. Alarm dissemination latency: In time of operational sufficiency.	TLR7
Risk management & incident management system **integration** (consolidation of real-time risk assessment with incident detection and management)	Innovative Solution	Improved risk assessment and containment: To level of operational sufficiency.	TLR7

Data input into advanced **dashboards** (dataset aggregation, mapping, and feeding into CIA/CIO dashboards)	Innovative Solution	Data compatibility: Op. sufficiency level. Degradation of dashboard responsiveness: To a level not degrading the op. sufficiency needed.	TLR7
Digital Instructional **Guides** (a series of interactive digital manuals with step-by-step guidance through risk and incident management across usability scenarios.)	Guidelines	User comprehension rate: To a level of operational sufficiency.	TRL7

1.1.2.6. Disruption Simulation & Preparedness Training [WP7&WP8]

Challenges: Serious games and disruption simulations play a crucial role in fostering **resilience thinking**[1] and **preparedness** within the context of critical infrastructures, considering all-hazard risks beyond just cybersecurity. Resilience thinking involves the ability to anticipate, prepare for, respond to, and recover from a wide range of unexpected and multifaceted challenges, including natural disasters, physical attacks, technological failures, and more. Serious games and simulations encourage participants to consider the interconnected nature of risks and the need for a comprehensive resilience strategy, facilitating cross-domain and cross-border collaboration.

Participants work together to address different aspects of a crisis, fostering an understanding of how diverse elements within an infrastructure system are interconnected and interdependent. These activities can be implemented through **board games, video games, digital twins, cyber ranges, or immersive experiences** (AR and VR); the common goal is to involve users in highly effective active learning experience. Resilience is a complex skill that is hard to acquire through conventional methods such as lectures and workshops. Active learning techniques such as gamification can provide solutions to this problem based on the emotional engagement produced by the challenges and rewards as fast feedback to learners. Serious games can extend **beyond organizational boundaries** to involve the broader communities. By engaging all different stakeholders in simulations, we raise awareness about all-hazard risks, promote community resilience, and encourage individuals to play an active role in emergency preparedness.

The Multi-Hazard Tournament (MHT), for example, is an emerging workshop methodology within the U.S. Army Corps of Engineers (USACE), which applies serious gaming and collaborative planning to the processes of learning and making decisions about multiple hazards that affect a particular area. Strategy and role-playing games like DisCoord allow to simulate the effects of weather events on the economy of small rural communities. In the Climate Adaptation Game, users are asked to make strategic decisions to mitigate the effects of climate change on their communities. Each action determines a specific evolution of the scenario. Through serious games and simulations, participants engage in holistic risk assessments that go beyond specific threats. They learn to identify relationships and dependencies, vulnerabilities, analyse potential cascading effects, and consider the broader implications of different risk scenarios, promoting a more comprehensive approach to resilience planning. Resilience thinking, moreover, involves effective decision-making under pressure. Serious games simulate high-stakes situations where participants must make critical decisions with limited information and time constraints. This enhances their ability to think strategically and make informed choices during real crises.

Ambition: We will **(i)** enhance the **awareness and preparedness** of CI authorities and operators in risk prevention and management through the use of serious gaming and simulation tools based on a **comprehensive (cross-x- and all-hazard-oriented) approach**. The innovative simulation tools will leverage a wide dynamic and multidimensional knowledge base, aiming to enhance the capability to thoroughly analyse the effects of known threats, including domino effects, and identify unknown threats beyond the scope of ordinary risk assessments. We will **(ii)** **improve the strategic decision-making** process through simulation practices. With an expanded context mapping, CI authorities and operators will enhance their ability to anticipate risks, enabling the adoption of more effective and efficient resilience strategies. We aim **(iii)** to boost the **adoption of the resilience thinking approach**, facilitating a re-skilling and up-skilling pathway through appropriate educational and training services on simulation tools.

Realisation: We will facilitate the adoption of resilience thinking, transcending traditional risk assessment, by **(i)** incorporating **active learning** methodologies into the training of CI operators. We aim to go **beyond the standard Cyber Range technology** and by merging it with the Digital Twin, we aim to create a virtual environment covering not only the digital infrastructure but also most Cis, **building a CI-Range environment for all essential service components**, serving a dynamic training environment. Serious

[1] https://www.mdpi.com/2071-1050/14/24/16760

games and CI-Ranges have the potential to engage stakeholders with novel and unexplored challenges, thereby promoting preparedness and fostering awareness of resilience. Additionally, we will **(ii)** cultivate a **collaborative mindset** to proactively mitigate risks and respond to disruption, both within cross-sector (MICRO and MESO pilots) and-cross border (MACRO pilot) scenarios, and **(iii)** provide training and education services to facilitate the **capacity building** of CI authorities and operators.

Result	Type	KPI & Target Value	Target TRL
Active learning & serious gaming methodologies	Methodology	**>70%** of registered users actively use simulation & training tools. **>80%** of active users report satisfaction score >4 out of 5.	TRL7
CI-Ranges	Innovative Solution	**>3** Essential services emulated in a virtual environment.	TRL7

1.1.2.7. Coordinated Cross-X (Stress) Tests & Large-Scale Exercises [WP9&WP10]

Challenges: Modern critical systems and infrastructures are deeply interconnected; a complicated network of dependencies and interdependencies can dramatically increase the impact of a critical event affecting a single CI. These dependencies involve both a functional and a spatial dimension; cross-sectoral interdependencies span several European countries. In order to deal with resilience of interdependent Cis, by raising the levels of prevention, preparedness, and response, **stress tests** and **joint exercises** need to be exploited. **Coordinated cross-X stress tests** can be seen as an advanced and cooperative way to **(i)** identify the operation limits and **(ii)** describe the vulnerabilities of a set of interdependent infrastructures in an international context. Coordinated Cross-X Stress Tests are aimed at raising preparedness of Cis' operators and their ability to prevent the impact of critical events. **Coordinated large-scale exercises** focus on the response provided by a large set of interacting actors (e.g., local, national, and international public authorities, CI operators, third parties) to a critical situation involving Cis. Exercises are focused on raising the preparedness and on smoothing the procedures in the communications between the different actors. Stress tests and large-scale exercises span both functional and spatial dependencies between Cis and can be adopted in an **all-hazard approach**, involving physical (e.g., earthquake, flooding) and cyber resilience (e.g., DDoS attack).

Coordinated stress tests and large-scale exercise play a crucial role in NATO's endeavour in testing and improving the resilience of Cis at a European and global scales. Locked Shields, organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), is one of the largest international cyber defence exercises; it focuses on simulating realistic and evolving cyber threats that a nation or organization might face, by involving attacking red teams and defending blue teams, involved in protecting the Cis and mitigating the effects. Similarly, Cyber Coalition emphasizes on cooperation and collaboration among different actors, involving participants from military, government, and industry, and fostering a multidisciplinary approach to cybersecurity. While these initiatives are essential for identifying weaknesses, improving preparedness, and raising awareness on interdependencies between Cis, they **require substantial resources and careful planning**. Conducting comprehensive stress tests involves significant financial investments. This includes the development of realistic and evolving scenarios, the deployment of specialized technology, and the coordination of various stakeholders in multiple entities (e.g., public authorities and operators). Coordinating exercises across different sectors **requires overcoming organizational silos, domain specific languages, and establishing effective communication channels**. Achieving seamless integration can be complex due to differing priorities and operational protocols. Regulatory compliance, data privacy, and data security add an additional layer of complexity to such tools.

Ambition: We will **(i) reduce the amount of resources** required by cross-x stress tests and large-scale exercises by optimizing and merging the efforts of CI authorities and operators across Europe and by designing **custom tests** that can be simulated using innovative technology (see Section 1.1.2.6), **(ii)** consider an **all-hazard, cross-x approach**, taking into account also the different **geopolitical, cultural, sectorial, and organisational aspects**, and **(iii)** identify **bottlenecks in communication and coordination** among different actors, that may impact the disruption response.

Realisation: We will overcome the identified limitations and reach our ambitions by **(i) designing** custom stress tests and large-scale exercises that cover all hazards, all critical sectors (as defined by the CER Directive), and all EU MS, and **(ii) executing** tests and exercises through different pilots that will include different project results (e.g., the strategy and different tools and services; see Section 1.2.3). Specifically, in the MACRO pilots, we will design stress tests that simulate complex, all-hazard and cross-x disruptions, allowing us to evaluate the effectiveness of our Disruption Resilience Strategy at a European level. In the execution phase, in running a selection of key tests and exercises, we will engage all consortium CI

authorities and operators, and beyond. Building on this, MESO pilots, situated in different EU MS and focusing on specific critical sectors, delve deeper into the localized challenges and interdependencies. Finally, the MICRO pilots offer a granular perspective, addressing resilience at individual sites, organizations, and regions. Through this hierarchical approach, we aim to create stress tests and exercises that cover a spectrum of hazards, account for diverse critical sectors, and reflect the unique vulnerabilities and strengths of each EU MS, thus ensuring a robust and all-encompassing evaluation of our resilience enhancing solutions.

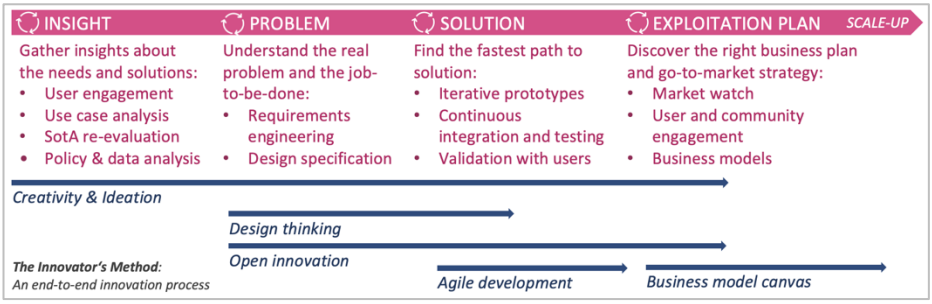
Result	Type	KPI & Target Value
Cross-x stress test designs and plans	Designs	**30+ stress test designs and execution plans** covering all-hazards, all EU MS, and all critical sectors (as defined by the CER Directive).
Large-scale exercises	Exercises	**3 large-scale exercises** (MACRO pilot) involving all project CIs and beyond covering all-hazards, 4+ different EU MS, and 6+ different critical sectors. **12 medium-scale exercises** (3 cycles of 4 exercises: MESO & MICRO pilots) covering key relevant hazards, 4 different EU MS, and 6 different critical sectors.

1.2. Methodology

1.2.1. Overall Methodology and Underpinning Concepts, Models, Assumptions

ENDURANCE focuses on **(i)** enhancing the **strategic cooperation and collaboration** among and across the EU MS CI authorities and operators, **(ii)** harmonising their **strategies** for disruption resilience, and **(iii)** delivering **data spaces, methodologies, technologies, and services** for joint assessment, anticipation, and management of risks, and interactive training on disruption resilience. In doing so, we will adopt a **user-driven approach** with a goal to **address concrete strategic and operational challenges of the CIs**. Following a **capability-driven methodology**, the end users will be deeply engaged in all key phases of the project in a **co-design and co-creation fashion** – from defining the capabilities they need and expect, to their final demonstration and validation.

We will follow the **Innovator's Method** (illustrated on the right), which includes a set of tools emerging from lean start-up, design thinking, and agile development concepts that are revolutionising how new ideas are created, refined, and brought to market via rapid experiments that lower failure risks.



Each step of the method (described below) is crucial and involves an experimentation loop to test assumptions in a repeated hypothesis-test-learn loop. Continuous questioning, observing, networking, and experimenting will be the catalysts of our success in delivering solutions for an unbiased, precise, efficient, and well-informed decision-making.

Gathering **INSIGHT**s	**Links to Objectives #1-#4 and WP1-WP4**

We will establish active cooperation mechanisms with the **end users / CI stakeholders** within the consortium and beyond (through the Working Group, the Advisory Board, and **WP11** activities) to understand the experience and best practices of various CI stakeholders, and to generate insights into their specific challenges and needs.

Desk research: We will look at **existing initiatives, datasets, policies, and approaches** for ensuring resilience of essential services against different threats, hazards, risks, and search for **ideas** across different best practices through an in-depth use case analysis [**WP1&WP2**], and an update to the here-presented SotA methodologies, technologies, services, and strategies for comprehensively understanding and effectively managing the European CI resilience [**WP3&WP4**].

Interactive workshops: With the baseline knowledge gained, we will **question the status-quo** and **capture the insights** directly from the end users in (national and European) thematic workshops based on **design thinking** approaches [**WP1&WP2**]. These will be organised in a **5-D format**, taking the participants through the steps of Defining, Discovering, Dreaming, Designing, and Developing the topic of CI resilience. Workshops will provide loads of information that we will consolidate, analyse, and formalise,

including the potential legal and ethical issues raised. Digital collaborative whiteboard platforms (e.g., Miro, Klaxoon) will be used for gathering and discussing insights.

Defining & detailing **PROBLEM**s	**Links to Objectives #2-#4 and WP3-WP8**

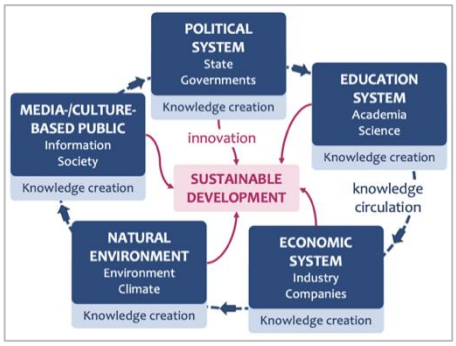
Once we have gathered the insights into the users' practices and available resources (data, technologies, strategies), and before we leap into building solutions, we will focus on deeply understanding **(i)** the **problems** (pains and desires) and **(ii)** specific functional and non-functional **elements** of the work to be done, leading to a detailed **roadmap**.

Requirement engineering & Design specification: Building upon the gathered insights, we will define, consolidate, prioritise, and maintain requirements for the ENDURANCE services [**WP3-WP8**], which will serve as a basis for all subsequent project activities. To define the requirements, design the associated building blocks, and prepare a detailed technical roadmap [**T3.5&T4.5**], we will adopt the **IIRA methodology** based on the following viewpoints:

- **Business viewpoint**: *Who are the stakeholders? What are their visions, values, and objectives? …*
- **Usage viewpoint**: *Who will be the users of our solutions? What is their expected use? ...*
- **Functional viewpoint**: *What are the structural components? What are their interrelations and interfaces? ...*
- **Implementation viewpoints**: *What activities and functionalities need to be implemented, and how? ...*

In doing so, we will rely on **design thinking** through which we will continuously seek to understand the users, to challenge the assumptions, and to redefine the problems to identify alternative solutions that might not be instantly apparent with our initial level of understanding. Specifically, we will follow two steps:

- **Pain-storming**: Generate hypotheses about a specific problem, identify the biggest pain points, conduct a root-cause analysis, identify assumptions behind the root causes, and test them with the end users.
- **Vision development**: Define a clear vision for each problem we will solve and test it with the end users.



Every problem has a functional, legal, ethical, social, and economic dimension. The importance of these elements varies across the use cases. Moreover, useful knowledge today is widely distributed. No organisation, no matter how capable or how big, can innovate effectively on its own. Therefore, we will align with an **open innovation** concept, and thus pursue a **multidisciplinary and collaborative** innovation approach.

Specifically, we will follow the **Quintuple Helix Innovation model** (shown on the right) to ensure that various perspectives from governments, industry, academia, and society are adequately considered in an **inclusive, co-creative, and collaborative manner**.

Developing & piloting **SOLUTION**s	**Links to Objectives #2-#4 and WP5-WP10**

After the problems are detailed, we will focus on finding the fastest path to solutions that best solve them.

Agile SW development: We will adopt an **agile SW development approach** as well as **Dev(Sec)Ops** and **DataOps** practices. We will build on the concepts presented in this proposal and on the baseline technologies of the consortium partners, to implement ENDURANCE-focused **basic prototypes** (tested in labs by **M18**, **TRL5**) and **minimum viable products** (tested and validated with users in relevant/operational environments by **M27**/**M36**, **TRL6/7**) – in this specific order, to reduce risks, shorten development cycles [**WP3-WP8**], and quickly validate results [**WP10**]. As an integral part of our commitment to (cyber)security, we will conduct comprehensive **penetration testing** at key development milestones to identify potential vulnerabilities, ensuring that our solutions are resilient to cyber threats.

CI/CD: A Continuous Integration/Continuous Deployment (CI/CD) environment will be setup and customised for project needs, and it will include well-known tools (e.g., Git) for source code management, Jenkins (or the like) for automated building and testing, Artifactory (or the like) for managing, storing, and distributing the produced binary files and others. The de-facto standards (e.g., Docker) will be used for bundling the software components.

Robust AI: Some of the ENDURANCE solutions are based on AI technologies. We will carefully design, implement, and thoroughly test [**WP3-WP10**] AI-based systems to ensure **technical robustness** (resilience to training and inference attacks, accuracy, reliability, reproducibility). We will integrate **human-**

in-the-loop (HITL) concepts in all phases of the data life cycle and deliver interactive AI-powered solutions. With the support of the SSH experts, we will ensure that our AI solutions are **socially robust** (duly consider the context and environment in which they operate) and are **generally safe** (explainable in decision-making and function as needed, safeguarding rights and integrity of humans). In this, we will follow relevant guidelines[2] and support the EU policy actions on AI.[3]

Establishing **EXPLOITATION & SUSTAINABILITY PLAN**s **Links to Objective #5 and WP11**

Once we've developed and tested the preliminary solutions with the end users, we'll be ready to define a mature exploitation & sustainability plan to get our results to the relevant scientific and policy-making communities (including competent authorities) and in the hands of the customers (including CI operators). To this end, we will experiment with the end users to discover the right business models, the optimal go-to-market strategy, and unique ways in which our future clients will discover, evaluate, use, and connect to our results.

Readiness assessment: To understand **(i)** the **impacts** our solutions may make, **(ii)** their **alignment** with the market needs, and **(iii)** the **likelihood** people will want to use them, we will regularly assess our solutions' technical readiness level (TRL), social readiness level (SRL), and societal embeddedness level (SEL) [**T11.4**,**T11.5**].

Business model canvas: We will conduct a market- and user-driven business development [**T11.4**] through continuous **market watch** and active **user engagement**. To prepare a scalable business plan, we will focus on the business model for each key result (in alignment with the established IPR agreements) [**T11.1**]. The main tool to be used for this, is the **business model canvas**, which captures all key business elements of a product: value proposition, pricing strategy, customer acquisition (relationships, channels), and cost structure (activities, resources). *See Section 2.2.2.*

We will continuously **promote** our results to different audiences to ensure uptake and follow-up [**T11.2**, **T11.3**].

Our methodology is designed in a way that it **does not harm biodiversity or climate**. We take due consideration to ensure that our solutions **respect the environmental objectives** of the EU Taxonomy Regulation **by design**. We will perform a continuous assessment of the impacts generated by ENDURANCE [**T11.5**], including those towards climate, to demonstrate **environmental and social sustainability** of our results.

1.2.2. Architecture

ENDURANCE will implement the foreseen capabilities, tools, and services by defining a distributed framework that integrates and exploits domain-specific (and/or operator-specific) risk assessment tools and delivers a cooperation-oriented approach to cross-X risk assessment based on the following **design principles**:

- **Flexibility**: Enhancing the ability of CIs to deliver essential services is paramount in addressing a wide array of risks, spanning natural and human-induced factors, accidental or intentional. This capacity necessitates a high degree of adaptability to accommodate emerging threats and scenarios, all while maintaining a robust and future-proof design and implementation.
- **Decentralization**: In the ENDURANCE ecosystem, the data, information, knowledge, and intelligence vital for resilience, are not centralized. Instead, they are generated, supplied, and accessible in a trusted federated environment. Data processing follows a decentralized approach, employing techniques such as federated machine learning.
- **Data sovereignty**: Ownerships and control of data are retained by providers/owners, subject to the laws and governance structures of the country in which they are located.
- **Security and trust**: The ENDURANCE ecosystem maintains confidence in the identity and capability (in terms of data and services) of participants and provides the measures and tools to protect the integrity and security of data and operations on them.
- **Specification**: Rules, specification, and protocols governing data, information, knowledge, and intelligence sharing as well as risk assessment within the ENDURANCE ecosystem, are agreed upon and specified.
- **Accountability**: Data, information, knowledge, and intelligence sharing and exchange are accountable.

[2] EC High-Level Expert Group's Ethics Guidelines for Trustworthy AI; ENISA's AI Cybersecurity Challenges; CNIL guidelines.
[3] EU's approach on AI excellence and trust.

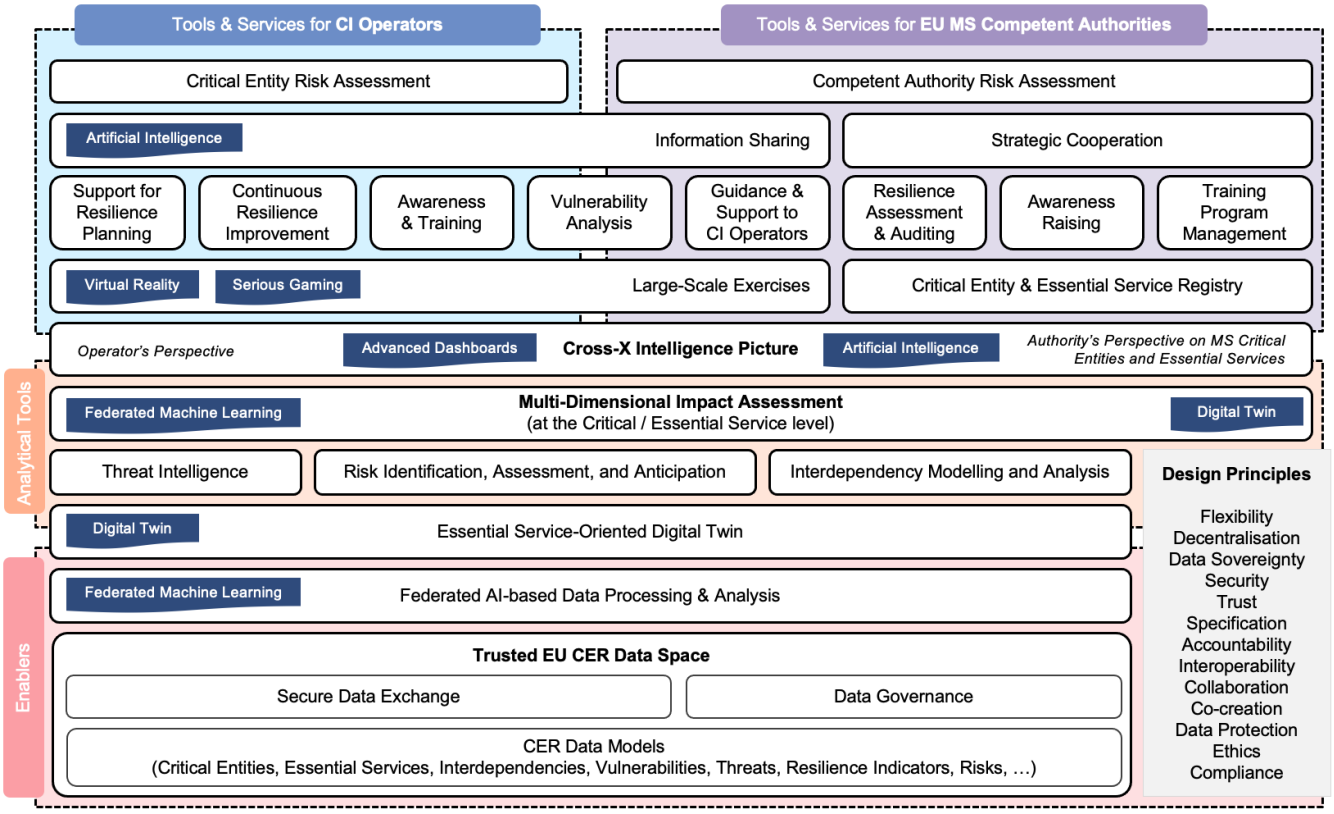
- **Interoperability**: The ecosystem enables various systems or services, including providers and users, to exchange and utilize harmonized research data, information, knowledge, and intelligence through standardized formats, structures, and semantics.
- **Collaboration and co-creation**: We recognize the value of co-creating knowledge and intelligence, fostering collaborative risk and resilience assessment and analysis. It provides tools to integrate and merge data and information for creating cross-X intelligence pictures and situational awareness, supporting interdependency-aware improvements in resilience.
- **Law and ethics**: Recognizing that the data may include personal, sensitive, and/or classified information, ENDURANCE operates in compliance with relevant legal and ethical rules, including privacy and data protection. It upholds fundamental rights and adheres to applicable legislations in EU Member States.

The **ENDURANCE Framework** (depicted below) is designed to provide advanced support to EU MS competent authorities and CI operators in their collaborative efforts for joint and comprehensive cross-x risk assessment and foresight. This framework encompasses data and intelligence sharing, and the facilitation of extensive resilience assessment and enhancement exercises. It consists of three primary macro-components, namely **(i) enablers**, **(ii) (risk) analysis and analytics** functionalities, and **(iii) specialized tools and services tailored for CI operators and/or authorities**. The ENDURANCE Framework leverages existing sector-specific risk assessment tools, ensuring that it aligns with the specific needs of different critical infrastructure sectors and operators. It represents a comprehensive and technologically advanced approach to risk analysis and resilience enhancement, strengthening the collaborative efforts of EU Member States in protecting CI and guaranteeing the provision of essential services.

Enablers [**WP5&WP6**]: The ENDURANCE distributed framework will be designed around three key enabling concepts and approaches, namely **data spaces** (supporting data sharing), **federated data analysis and machine learning** (supporting data sovereignty and collaborative analytics), and **digital twins** (supporting modelling, analysis, and simulation), as further elaborated below.

Trusted EU CER Data Space. We will go beyond secure data exchange for supporting the cross-X risk assessment and resilience analysis by creating the foundations for a trusted, sustainable, and accountable Data Ecosystem, that complies with European values and principles on data protection, privacy, ethics, enabling and supporting multiple data spaces, where interested actors (i.e., operators, authorities) deposit, share ,and co-produce data and intelligence on the resilience of CEs, based on common rules, protocols, standards, and tools in a trusted environment and accompanying governance framework. Common schemas for data exchange will be defined, considering the European dimension and possible differences among the MS (e.g., in the definition of CEs and essential services).

In designing the Trusted EU CER Data Space, we will leverage on relevant EU initiatives and reference architectures for Federated and Secure Data Infrastructure (i.e., GAIA-X) and Data Spaces (i.e., IDSA) as well as expertise within the INFRA community, of which most consortium partners are an integral and longstanding part. We will specialize these concepts to address the particular needs of data spaces for CER data and intelligence such as high sensitiveness of data, strong ethical and legal challenges including societal sensitivities, cross-border dimensions, purposes of data sharing (e.g., cross-X risk assessment) as well as potentially conflicting interests (e.g., between operators, in different countries). We will adhere to the principle of proportionate information sharing. The exchange of information will be confined to what is pertinent and necessary for the specific purpose of that exchange. This approach ensures the confidentiality of information, safeguarding the security and commercial interests of critical entities. Simultaneously, it upholds the security protocols of Member States.



Federated AI-based Data Processing & Analysis. We recognize the impossibility of full data sharing due to (security, business) sensitiveness of data (containing information about infrastructure configurations, vulnerabilities, and potential risks) and cross-border dimension. Therefore, we envisage and encourage a decentralized approach to data processing and analysis aimed at assessing cyber and physical risks in networks of interdependent CEs. Thus, while Machine Learning (ML) techniques will be exploited for analysing data to identify patterns, vulnerabilities, and potential risks as well as to predict and prevent incidents that could impact CI, we will adopt federated ML (FML) for risk analysis in critical infrastructure protection and resilience, as a cutting-edge approach that harnesses the power of ML while addressing the sensitive nature of data in the context of safeguarding vital infrastructure.

With FML, collaborating parties (e.g., infrastructure operators or authorities) retains control of their data, keeping it on-premises or within its jurisdiction. Instead of sharing data, the parties share ML models or algorithms. These models are trained locally on each party's data. Periodically, the parties exchange model updates or gradients without sharing the underlying data. The global model learns from the local models while maintaining data privacy. Sensitive data remains protected within each organization's boundaries, addressing data sovereignty and privacy concerns. However, parties will be able to collectively analyse data and build robust ML models without exposing their data to external threats. By analysing data from multiple sources, FML can provide a more comprehensive view of potential risks and vulnerabilities.

We will design and deliver an FML-based infrastructure that will enable federated data analysis and collaborative analytics on multiple use cases related to CER, such as threat identification and intelligence, vulnerability identification and analysis, risk assessment, impact assessment, resilience assessment and analysis, predictive analytics on risks, prescriptive analytics on countermeasures, etc.

Essential Service-oriented CER Digital Twins (DT). We will adopt a DT methodology to model and scrutinize risks impacting the resilience of critical entities within cross-X environments, particularly emphasizing essential and critical services provided by these entities. These DTs will intricately simulate and represent systems or intricate networks interconnecting Cis collaborating to deliver vital services to society. The focal point of our DTs will be on delineating relationships, interactions, and dependencies among critical entities, aiming to evaluate the resilience and reliability of essential services while understanding the broader impact of disruptions or alterations in a single critical entity on the entire essential service network.

The framework for constructing and analysing **DTs cantered on essential services** will be bas on the EU-funded PRECINCT project, especially in terms of interdependency modelling. This framework will

encompass the essential services dimension, enhancing its applicability to the intricate landscape of interconnected critical entities.

The framework will facilitate the modelling of concepts, criteria, and information, encompassing elements such as the user base reliant on essential services offered by the pertinent entity, the degree of dependence of other critical entities (across various sectors and subsectors) on the specified essential services, the potential impact of incidents on economic and societal activities, environmental aspects, public safety and security, and population health. Additionally, it will consider the geographic scope affected by an incident, incorporating cross-border implications. The framework will also evaluate the entity's significance in sustaining an adequate level of the essential service, accounting for the availability of alternative means for service provision.

Analytical Tools (for risk analysis) [**WP5-WP8**]: The identified key enablers will serve as the technological and methodological foundations for the ENDURANCE analytical capabilities for enhanced risk assessment and analysis.

Threat Intelligence. We consider a dynamic threat landscape, which includes evolving hybrid and terrorist threats, the increased physical risk due to natural disasters and climate change, both cyber and physical threat. All these threats can reduce the capacity, efficiency, and lifespan of certain infrastructure if appropriate measures are not in place. To address such a complexity and dynamics, we will support the collection and analysis of data and information to extract insights related to potential cybersecurity threats and physical risks that could impact essential services and critical infrastructure. The ENDURANCE threat intelligence will be based on the following key features, to stay ahead of emerging threats and vulnerabilities, helping to maintain the reliability and security of essential services: enhanced and richer data and knowledge on threats, incidents, vulnerabilities, attacks, attributions, etc. (within CER data spaces) and augmented analytical capabilities based on collaborative intelligence (supported by FML). We will also deliver novel data collection and analysis tools for threat intelligence based on dark net information.

Interdependency Modelling & Analysis. Due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Thus, leveraging on the Digital Twin approach to essential service modelling, ENDURANCE will deliver tools and primitives for modelling and analysing the interrelationships and dependencies between different critical entities and infrastructures, showing how disruptions or failures in one part of the network can impact others. This modelling helps in understanding the cascading effects of disruptions.

Given the rising interconnectedness and transboundary character of critical infrastructure operations, protecting individual assets is insufficient to thwart all potential disruptions. Therefore, by harnessing the Digital Twin methodology in modelling essential services, we aim to define and provide tools and foundational components for modelling and scrutinizing the intricate interconnections and dependencies among diverse critical entities and infrastructures in relation to their provision of essential services. This modelling will support the analysis of how disturbances or breakdowns in one segment of the network can reverberate throughout others, facilitating a comprehensive understanding of the cascading effects of disruptions.

Starting from existing sector-specific risk assessment and analysis systems and services, we will leverage on the key enablers to deliver "improved" **Risk Identification, Assessment & Anticipation** capabilities that will benefit from trusted data sharing (i.e., data spaces), collaborative analysis and intelligence (i.e., FML) and interdependency and service-oriented modelling and simulation (i.e. digital twins). Specifically, this module will comprise a cohesive set of analytical components operating within an augmented data space. This space, incorporating cross-entity essential service interdependencies, threat landscapes, vulnerabilities, etc., will facilitate advanced multi-dimensional analytics on specific resilience indicators. The aim is to achieve more robust and integrated risk identification, assessment, and anticipation.

Multi-level Impact Assessment. Based on threat intelligence, identification, assessment, and anticipation of risks, and CEs and essential services interdependency modelling, we will define and deliver capabilities for evaluating the potential consequences and effects of various scenarios, events, or threats on different levels of CI and their service provisioning. Proactive approach to understanding and mitigating risks. This includes scenario analysis, by which various threat scenarios are developed and analysed, ranging from localized incidents to large-scale disasters. By considering the effects of various scenarios on different levels of infrastructure, authorities can better prepare for and respond to potential threats, thereby ensuring the continuity of essential services and the safety of communities.

The bridge connecting ENDURANCE's analytical capabilities to the services designed for operators and authorities is the **Cross-X Intelligence Picture**. This sophisticated tool serves as a holistic and ever-evolving representation of the security and risk landscape. It employs advanced dashboards and various forms of intelligence and data visualization to facilitate informed decision-making and risk management.

The ENDURANCE Cross-X Intelligence Picture services will consolidate, structure, and present information in a format that aids in comprehending potential threats to CEs and CI. This includes data related to vulnerabilities within these critical entities and infrastructure, historical records of incidents, breaches, disruptions, or attacks on them. It also assesses the likelihood of different threats occurring and their potential impact on operations. The tool provides insights into potential threat actors, identifies emerging trends that could pose risks to critical infrastructure, and visualizes this information through maps, timelines, graphs, and other data visualization techniques.

The baseline capabilities for data acquisition, processing, and sharing, service-oriented digital twins, collaborative and federated risk analysis and analytics will be integrated into **two set of user-drive services respectively for CI operators and for authorities** responsible for resilience on national level of for overseeing those operators. Some of the services are **common to both families of end-users**, such as **Large-Scale Exercises**. We will provide a European environment based on simulation, serious games, and virtual reality to plan, perform, monitor, and analyse resilience assessment exercises involving multiple CI operators, at the regional or national level or cross-border. These exercises play a crucial role in enhancing the preparedness of CI operators and authorities to address potential threats and disruptions. Leveraging on the above-mentioned cutting-edge technologies, these exercises can provide a comprehensive and immersive environment for multiple CEs to participate and test their resilience strategies.

Serious games are interactive and engaging scenarios that replicate real-world situations. In the context of resilience assessment, these games will simulate various crisis situations, including cyberattacks, natural disasters, or other disruptions. Multiple CE operators will participate in these games to evaluate their response strategies and decision-making processes, with a strong focus and attention to interdependencies and cascading effects. Through gameplay, participants gain valuable experience and insights into how to manage complex incidents effectively.

Resilience assessment exercises may involve large-scale *simulations* of crisis scenarios leveraging on the essential service-oriented digital twins representing CEs and the interdependencies among them. Authorities and operators will use such simulation tools to replicate the behaviour of such complex networks during disruptive events or in response to them. Multiple CI operators and authorities will collaborate within a controlled environment to understand the potential cascading effects and assess their collective response capabilities. Simulations provide a risk-free space for operators to test different strategies and make informed decisions.

Virtual reality technologies will provide the immerse digital environment that replicates real-world conditions when recreating emergency situations. Collaborative VR experiences facilitate joint exercises involving multiple CI operators and authorities who can interact and coordinate their actions in a virtual crisis scenario.

The strength of resilience assessment exercises lies in their ability to engage various critical infrastructure operators and various authorities involved in the resilience of critical entities at the regional, national, or European level. These exercises bring together operators from different sectors and industries to jointly address complex challenges. By involving multiple stakeholders, authorities and operators can gain a more comprehensive understanding of interdependencies, foster cross-sector collaboration, and test their collective resilience strategies.

Resilience assessment exercises based on these technologies promote experiential learning and provide operators with valuable insights into their readiness to tackle disruptive events. By embracing innovative tools and involving multiple operators, these exercises contribute to the development of robust and adaptive strategies for ensuring the continuity and security of essential services.

We will also define a deliver a collaborative approach to **Vulnerability Analysis**. It will be encapsulated into a service for both operators and authorities that integrates and exploits the augmented and collaborative information space including threat intelligence, interdependency analysis and specific critical entity configurations to deliver and keep updated a vulnerability map aimed at identifying (potential) weaknesses and susceptibilities in CEs and network of interdependent CEs.

Within the Trusted EU CER Data Space, we will provide capabilities and services for **Secure Information & Intelligence Sharing** on CE resilience and risks, in accordance with EU and national law on, in

particular, classified and sensitive information, competition and protection of personal data. The ENDURANCE services will support information sharing among CEs, between CEs and competent authorities, and among competent authorities with the same MS (in case the MS establishes more than one competent authority) by utilizing innovative “by design” solutions such as Zero Trust Network Access (ZTNA) and federated utilization of data and information without moving sensitive or classified data via Zero Trust FML (ZT-FML) techniques.

A fundamental service in the context of information sharing is the *notification of relevant incidents* by the CE to the competent authority to generate a comprehensive overview of the impact, nature, cause, and possible consequences. This service will support CE in notifying the competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. The notification will include the information to make the competent authority aware of the incident and, where possible, the presumed cause of the incident, followed, where relevant, by a detailed report with a more complete overview of the incident. Across the same information channel, the competent authority can provide the critical entity concerned with relevant follow-up information, including information that could support that critical entity’s effective response to the incident in question.

Competent authorities will also be provided with additional service supporting the **Information Sharing & Strategic Cooperation** with the corresponding authorities in other MS (and potentially with other European bodies, e.g., the Critical Entities Resilience Group). Such services will enhance their ability for cooperation and communication, in the context of large-scale, cross-border risk assessments developing and sharing best practices and guidelines. This is the case of CI connected to two or more MS, or linked to / depending on / providing services to other MS.

Specific **ENDURANCE Tools & Services for EU MS Competent Authorities** [**WP7&WP8**] include:

- **Member State risk assessment**: According to the CER Directive, “each MS should carry out, within a harmonized framework, an assessment of the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, that could affect the provision of essential services”. We will integrate and deliver a service to support competent authorities to perform risk assessment at the MS level, taking into account general or sector-specific risk assessment and the interdependencies among the sectors.
- **Critical Entity & Essential Service Registry**: We will design and deliver a prototype of cyber-secure data and knowledge management system for collecting, storing, and managing sensitive information on CEs and their essential services at the national level (i.e., that operate and have critical infrastructure located on its territory). This will represent the informative foundation for implementing the CER guidelines at the national level. This service is not only a registry, but also a support to identify CEs according to the CER Directive and exclude those entities and services which are not covered by it (e.g., defence, law enforcement, national security), following a risk-based approach that focuses on the entities most relevant for the performance of vital societal functions or economic activities. The identified CEs will be subject to specific requirements and supervision and that will be provided with particular support and guidance in the face of all relevant risks. This service will also support the competent authority in reporting the EC on national essential services and CEs.
- **Guidance and Support to CE operators**: We will deliver a set of coherent and integrated informative services, managed and provided by the competent authorities, to support operators in improving the resilience of their CEs, according to the strategy. Set at the national level. This will include tailored guidelines, recommendations, assistance, Q&A, etc., to meet the obligation imposed by the CER Directive and national law.
- **Resilience Assessment & Auditing**: We will design and deliver a service to support the competent authorities in their processes for assessing and auditing the resilience of the CEs under their scope and overseeing, in terms of fulfilment of their rules and obligations resulting from the CER Directive. This will include process automation to establish whether risk assessment carried out by a critical entity is compliant, in whole or in part, with the obligations laid down in this Directive.
- **Awareness Raising**: We will deliver a service to create and configure awareness campaigns on resilience, CER directive, recommendations and obligations, targeting CE operators and other relevant stakeholders.
- **Training Program Management**: We will deliver a service for the preparation and management of training programs on resilience for CE operators.

Specific **ENDURANCE Tools & Services for CI operators** [**WP7&WP8**] include:

- **CE Risk Assessment**: We will provide novel capabilities to critical entities to support their comprehensive understanding of the relevant risks to which they are exposed and to analyse those

risks. This will be done based on MS risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services. This service will provide a CE-cantered perspective on information, knowledge and services offered by the ENDURANCE analytics tools (threat intelligence, risk identification and anticipation, interdependencies, impact analysis), complemented with the specific information of the considered CE, integrating the insights resulting from the large-scale exercise.

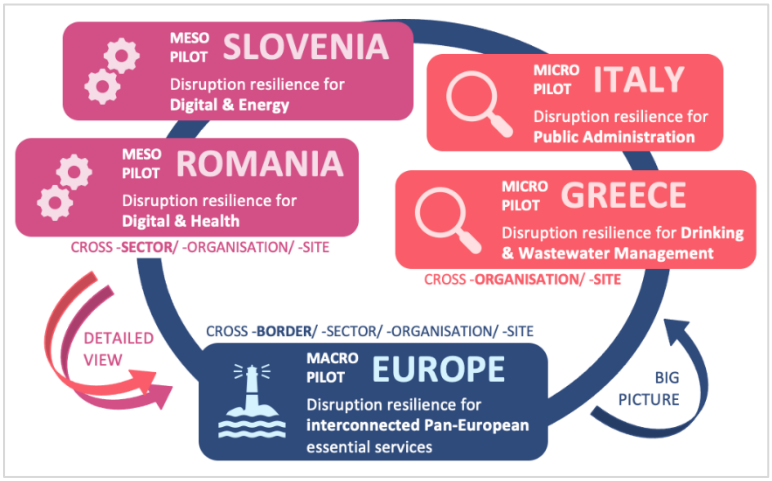
- **Support for Resilience Planning**: We will deliver a service supporting and assisting CI operators in the creation and updating of their resilience plans, considering the joint risk assessment, enabled, and supported by the overall ENDURANCE Framework and its services. This service will help them to comply with the CER-Directive.
- **Continuous Resilience Improvement**: We will provide an analytical service for post-exercise results analysis. This service will help operators in figuring out relevant insights from those large-scale exercises, in terms of additional threats, vulnerabilities, and risks to consider and potential measures to adopt to mitigate them.
- **Awareness & Training**: We will provide the operators with a set of coherent services to use the awareness and training campaigns and contents organized by the authorities through the services described above.

Note that the set of services for operators and authorities could be slightly redefined or reorganized during the project according to emerging needs and based on the planned detailed requirements and needs analysis.

1.2.3. Pilot Studies

All project outcomes will be **co-created and evaluated** in relevant settings with a variety of CI authorities and operators from different EU Member States, thereby preparing the results for a real-world uptake across different critical sectors and countries.

As illustrated below, we define a **3-layered piloting approach**: The MICRO pilots in Italy and Greece will capture the specificities of the individual countries, regions, and sectors focusing on the **cross-organisation and cross-site** aspects. The MESO pilots in Slovenia and Romania will identify, analyse, and address the **cross-sector** challenges on a local, regional, and national level. The large-scale, pan-European MACRO pilot will capture, understand, and tackle challenges on a **cross-border, European**, **strategic** scale.

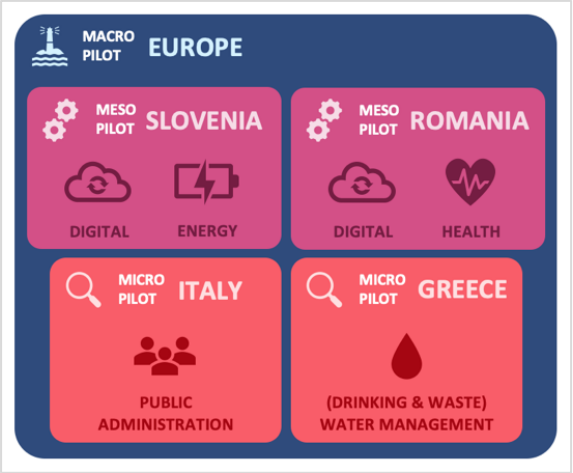


Pilot complementarity: Each pilot involves at least one competent national / regional / sectorial CI authority and at least one public / private operator of essential services. Moreover, each pilot covers at least one critical sector and at least one EU Member State. By assuming different levels of granularity and different angles, the pilots are highly complementary in the sense of gathering and exchanging detailed operational perspectives and high-level strategic views. Specifically, the MACRO pilot is strategically oriented, dealing with high-level, cross-border challenges, while the MESO pilot operates on a more practical, operational level with a selection of critical sectors. The MICRO pilot, in contrast, is highly focused and validation-oriented, examining the fine details.

All pilots together facilitate a **holistic approach** (as illustrated on the right): The MACRO pilot is setting the strategic vision and serving as a lighthouse, thus influencing / shaping the overarching policies and directions. The MESO pilot is translating the strategic goals into practical actions on an operational level. The MICRO pilot is highly focused on fine-tuning and validating small-scale and specific aspects. In turn, the MICRO pilot is providing feedback in terms of specific operational challenges, the MESO pilot is highlighting the strategic gaps, and the MACRO pilot builds on the insights and experience to improve the policies. This 3-tiered approach that **integrates the**

bottom-up and top-down perspectives, is allowing for a comprehensive assessment and improvement of the status quo, is enabling a structured progression from high-level strategy to practical execution, and vice versa by integrating experience from the operational level into policies.

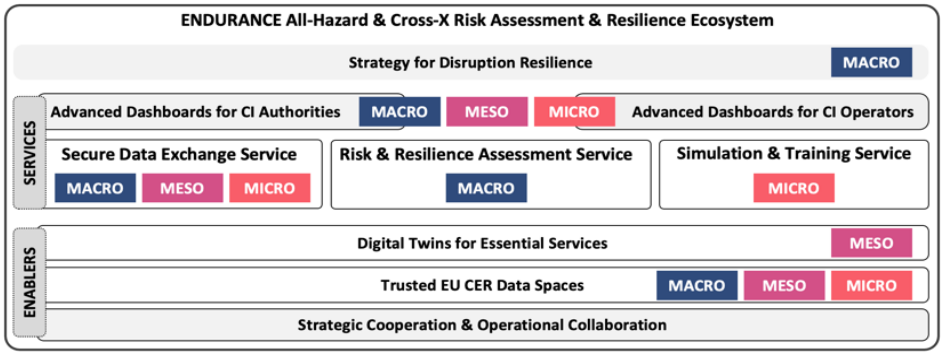
Pilot scope: As shown on the right, the MICRO pilots will focus on the resilience of the (physical, cyber, and human) enablers of the **Public Administration** and **(Drinking & Waste) Water Management** services. They will focus on the disruptions that stem from **(1)** the heterogeneous distribution of their own resources across different (physical and digital) sites (including different regions) and **(2)** the complex networks of (public and private) organisations involved in the supply chains their essential services interface with. The MESO pilots will extend to a broader set of critical sectors and will focus on the resilience of vital services in the **Digital, Energy, and Health** sectors from the perspective of cross-sector interdependencies and cascading effects of disruptive events like **(1)** electricity blackouts resulting in disruptions in telecommunication services, **(2)** digital blackouts resulting in disruptions in the electricity distribution and/or the provision of the basic healthcare services, and **(3)** large-scale health emergencies resulting in critical failures the digital infrastructure, emphasizing the intricate interplay between the availability of the human resources (workforce) and availability of other essential services (in our case, digital). In this way, the MESO pilots aim to comprehensively address the challenges arising from the convergence of CI sectors. The MACRO pilot serves as the overarching framework for all these efforts across **Europe**, synthesizing insights and knowledge across **all above-mentioned sectors and regions** to develop a unified and comprehensive pan-European strategy for addressing complex resilience challenges (and compliance with the associated legal framework in the form of the CER, NIS2, and other sectorial policies). This pilot focuses on cross-border, -sector, -organization, and -site collaboration and harmonisation to enhance the resilience of the European Cis in the face of a wide range of hazards and threats, ensuring the continuity of essential services and safeguarding the well-being of communities across the EU.



All-hazard approach: The pilots will demonstrate and evaluate the ENDURANCE strategy and services in the context of **all types of threats and hazards** to which Europe is exposed. The specific threats and hazards to be put in the forefront of each pilot **may vary** depending on the sectorial specifics (e.g., cyber threats are most relevant for the digital services while natural disasters more significantly affect water management), geographical location (e.g., areas near fault lines are more prone to earthquakes while inland areas are more exposed to floods), and other relevant aspects like, for example, the current global context and community demographics.

The list of here-presented threats and hazards will be **revised** (**T5.1, T6.1**), following a continuous dialogue with competent CI authorities and operators across Europe and CER experts from different disciplines to ensure that the **resilience strategies remain adaptive and relevant** to the evolving risk landscape, safeguarding the European interconnected essential services against both known and emerging threats. This collaborative approach ensures that the resilience framework **remains robust and responsive** to the unique needs and challenges of the CI in different geographical locations and operational contexts.

With this, ENDURANCE will **improve Europe's collective capability to anticipate and understand future risks and possible disruptions, and adapt risk management practices, strategies, and policies accordingly**.



Benefits to be demonstrated and validated (**KPIs are in Sections 1.1.2 and 2.1**): With all the pilots, our common goal is to **demonstrate and validate the benefits of the ENDURANCE results**: **(1) Increased collaboration and cooperation** among relevant public and private stakeholders, across sectors and national / regional borders, at all levels (strategic and operational). **(2) Strengthened governance framework** and improved coordination among the different national / regional / sectorial CI authorities. **(3) Efficient identification** of essential services, critical entities, and the known and emerging threats, hazards, and risks. **(4) Unified approach to (strategic and operational) cross-x risk and resilience assessment**, considering interdependencies and all types of threats / hazards. **(5) Harmonised understanding and implementation** of the relevant European / national / sectorial legislation on resilience (e.g., CER and NIS2 Directives). **(6) Skilled and security-aware personnel** in organisations responsible for the operation and oversight of essential services. **(7) Jointly tested strategy and services** for the all-hazard analysis, business continuity, and personnel training. **(8) Improved preparedness, response to, and recovery from** all-hazard disruptions of essential services. **(9) Greater economic stability and societal preparedness**.

Piloting process: Building on the results of the »pre-piloting activities« [**WP1-WP8**] involving **(1)** the identification of essential services, critical entities, and interdependencies, **(2)** the assessment of vulnerabilities, threats, hazards, risks, and potential cascading effects of disruptions, and **(3)** the development of the strategy and services for the cross-x, joint risk and resilience assessment, the **piloting activities** assume the following core tasks, illustrated on the right [**WP9&WP10**]:

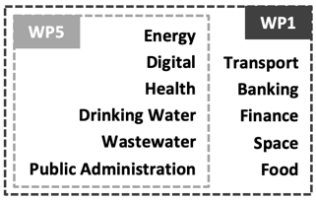
- **Re-evaluating** the specific threats and hazards relevant for each pilot given the (then) current local and global context.
- **Refining the scenarios** for the validation of result to capture realistic challenges and user needs based on the defined / chosen threats and hazards.
- **Integration of (1) services** enabling secure data exchange and federated processing, risk and resilience assessment, digital twins, and training, and **(2) strategy** (for business continuity and disruption resilience) from **WP1-WP8** into the relevant / operational environments of the users.
  - For service integration, this task involves the development of custom interfaces. Our technologies will be pluggable and offering REST APIs, thus reusable by any service in any pilot.
  - In terms of strategy integration, we will update and align the existing practices, guidelines, and business continuity plans with the ENDURANCE strategy (covering, risk assessment methodologies, disruption management approaches, and crisis communication protocols, among others).
- **Training** of the end users' employees on the use of the ENDURANCE services and strategy.
- **Validation** of the services and strategy through different **real-world scenarios**. Initially, we will deploy the technologies in **lab environments** and conduct thorough **testing** to ensure they meet the required functionality, security, interoperability, and usability (**TRL5** at M18). Building on the feedback from this initial validation and subsequent improvements, we will deploy the technologies in **relevant / operational environments** and demonstrate the expected functionalities and benefits (**TRL6** at M27, **TRL7** at M36).

To efficiently distribute the resources while ensuring that all our results are demonstrated and validated in the most relevant environments, different pilots will primarily focus on one specific service (while all pilots will test the new **Trusted EU CER Data Spaces**, **Secure Data Exchange Service**, **Advanced Dashboards**) as illustrated on the right:

- MICRO: The **Simulation & Training Service** to evaluate usability (incl. completeness and clarity).
- MESO: The **Digital Twin** to demonstrate the cross-sector interdependencies.
- MACRO: The **Strategy** and the **Risk & Resilience Assessment Service**, to **directly support the CI authorities and operators in the implementation of the CER Directive**.

In each pilot study, we have **representatives of public and private domains** (government authorities with domain expertise, public and private end users with data and relevant experience, and technology providers) that will actively participate in the **co-creation** of pilot studies and **evaluation of the relevance and value** of the project results.

Scalability to other CER Sectors and EU Countries: The critical sectors directly covered by the involved end users and pilots (Energy, Digital, Health, Drinking Water, Wastewater, Public Administration) represent **over half (6/11) of all sectors** as per the CER Directive. We directly cover 4/28 EU MS (Slovenia, Romania, Italy, Greece). But we do not stop here: **(i)** Since all critical sectors depend on electricity and digital services, directly considering these two sectors provides an important baseline upon which we can easily **scale to all other domains**. **(ii)** In the process of gathering inputs for the project work and evaluating results, we will (in the scope of the Working Group and workshops with the authorities and operators in **T1.1&T2.1**), **extend our research also to all other critical sectors** (Transport, Banking, Finance, Space, Food; see on the right) **and other EU MS**.



1.2.3.1. MACRO Pilot EUROPE [led by INS in T9.1&T10.1]

Strategic cooperation and operational collaboration among the CI authorities and operators are essential because in the interconnected landscape of critical infrastructures and essential services, a disruption in one sector and/or country can quickly cascade across others. To strengthen the resilience of the European CI and essential services they offer, it is imperative to have a **shared list of critical entities** and a **unified definition of a disruptive event**. Moreover, it is critical to have a **holistic understanding** of the potential vulnerabilities, threats, and risks that may emerge from **(i)** the interdependencies across different sectors and countries, **(ii)** sector-/country-specific **policy disparities** that can introduce complexities and uncertainties that affect the overall European CI resilience, and **(iii)** sector-/ country-specific **disruption management differences** that result in sub-optimal response and communication. For example, if one country's policies and procedures for disruption preparedness and response significantly differ from those of a neighbouring country, this misalignment can lead to inefficiencies in cross-border crisis management and can hinder the smooth cross-country coordination necessary during large-scale disruptions. Similar challenges appear on the sectorial level. An approach that works well in one sector might not be suitable for another, potentially leading to vulnerabilities when sectors interact or rely on one another. The **ENDURANCE Strategy for Disruption Resilience** will harmonise the definitions and procedures across sectors and countries, and thereby **(i)** address challenges created by the above-mentioned variations, **(ii)** enhance understanding of the cross-x risks, and **(iii)** enhance the preparedness of CI authorities and operators to anticipate and effectively manage disruptions.

Further, apart from **strategic cooperation** that assumes the harmonisation of the definitions and procedures, it is vital to also **enhance operational collaboration** and close collaboration **across both levels**. Specifically, for an effective anticipation and assessment of risks and potential cascading effects, a **Trusted EU CER Data Space** is needed within which CER-/risk-relevant data can be **securely shared** among the CI authorities and operators (or processed in a privacy-aware federated manner when sharing isn't possible). This enhances situational awareness across borders and sectors and provides reliable means for a more structured and standardized approach to evaluating the robustness of the CI in the form of a joint, cross-x, and real-time **risk and resilience assessment**.

This pilot brings together **all CI authorities and operators** engaged in the project (and beyond). It serves as a vital platform for testing and validating the ENDURANCE Strategy, Trusted EU CER Data Space, Secure Data Exchange Service, Risk & Resilience Service, and Advanced Dashboards. The MACRO pilot EUROPE thereby stands as a **testament to the commitment of the (engaged) CI authorities and operators to safeguard Europe's CI**.

1.2.3.2. MESO Pilot SLOVENIA [led by ICS in T9.2&T10.2]

In today's rapidly evolving European landscape, the CI operators are at the forefront of a digital transformation. This transformation, driven by the proliferation of Internet of Things (IoT) and the integration of Artificial Intelligence (AI) into control and monitoring systems, promises remarkable

improvements in efficiency. However, it also presents a fundamental shift in how the Cis function. The convergence of these digitally driven systems, spanning various sites, organizations, and even sectors, introduces unprecedented opportunities for seamless integration across the supply chain but, at the same time, widens the attack surface. Cyber threats, both subtle and sophisticated, as well as physical attacks and natural or man-made disasters, now have the potential to disrupt every facet of CI operations, impacting power generation, power transmission, power distribution, telecommunication services, and more.

In this pilot, we focus on the **interconnected vulnerability of the Energy and Digital sectors, considering the symbiotic relationship in the context of the digital transformation**. The energy sector heavily relies on seamless communication services for the precise management of power generation, transmission, and distribution. In the event of a **cyber-attack disrupting these communication channels**, the ramifications are profound. For instance, a well-coordinated attack targeting the communication infrastructure could impair the energy sector's ability to monitor and regulate the power flow, potentially leading to widespread blackouts and energy supply instability. Conversely, within the telecommunications sector, which forms the backbone of modern connectivity, a growing spectrum of cyber threats looms. These threats aren't confined solely to external actors but extend to users within the energy sector. Consider a scenario where a **compromised energy operator inadvertently introduces malware** into the telecommunications network while accessing services. Such an incident jeopardizes the integrity of data, raises privacy concerns, and endangers the availability of vital communication services. These consequences, when left unchecked, can escalate beyond the realm of economic disruption, affecting public safety and even national security. The challenges posed by this digital transformation and increased interdependence demand a radical shift in risk perception and, more critically, underscore the need for a transition to more agile risk management approaches capable of timely and effectively recognising, understanding, and countering evolving threats. Similar examples of disruptions that propagate from one sector to another can be found for cases of **physical attacks or natural-/human-made disasters**. Severe floods in a wider area (as has happened in Slovenia in August 2023) that damage the physical infrastructure of an energy provider and incapacitate their services for a longer period of time can render local telecommunication services that rely on the provision of power unavailable. This pilot will study all such cases that are most pressing for both sectors from the perspective of their interdependence.

This pilot is a collaborative initiative involving **2 national and sectorial authorities** and **2 key CI operators**: **URSIV**, the **national authority for the digital sector**. **AKOS**, the **sectorial authority for the digital sector**. **TS**, Slovenia's largest **telecommunications service provider** as well as the leading and most advanced Slovenian provider of cutting-edge ICT services and solutions (including SOC services to various stakeholders in the private and public sector). **ELES**, the operator of Slovenia's electric power transmission system, which is closely connected to the transmission networks of neighbouring countries and integrated into the European energy system.

1.2.3.3. MESO Pilot ROMANIA [led by EVI-RO in T9.3&T10.3]

Critical infrastructure and essential services are the backbone of modern society, and their proper functioning is crucial for the well-being of citizens. **Increasing the level of service digitization** is one of the goals in all sectoral development plans in Romania. But beside all benefits of remarkable evolution of digital technologies, digitalization increased the interconnectivity of critical systems, introduces complexities and potential vulnerabilities. Securing these interconnected systems is a continuous challenge to overcome, as well the evolution of the threat landscape, which includes a wide range of threats, including cyber-attacks, natural disasters, terrorism, aging infrastructure, supply chain disruption, human factors or resource constrains.

Our attention will be directed towards the **interdependent vulnerability of the Health and Digital sectors in Romania**, examining their symbiotic relationship within the framework of digital transformation and sustainability.

Several key aspects illustrate this interconnection between these two domains:

- Digital technologies play a crucial role in managing health information, **electronic health records (EHRs**), and **healthcare data**. The digital sector provides the tools and infrastructure necessary for efficient storage, retrieval, and sharing of health-related information, promoting interoperability among healthcare systems.
- Expansion of **telemedicine and telehealth** services, allowing healthcare professionals to remotely diagnose, monitor, and treat patients. This benefits both sectors by increasing accessibility to healthcare services and optimizing resource utilization.

- The **Internet of Things (IoT**) facilitates the connection of medical devices and equipment, enhancing real-time monitoring and communication between healthcare systems.

As healthcare systems increasingly rely on digital technologies, ensuring the security of patient data and healthcare infrastructure becomes crucial. The digital sector contributes with **cybersecurity solutions** to protect the sensitive health information and infrastructure. In a hypothetical scenario, of **compromise the for a** during a cyberattack, the situation opens the ground for several risks and potential consequences such as data integrity compromise, privacy breach, disruption of Healthcare Services, compromised patient safety, reputational damage, operational disruptions. The incident could have lasting effects on the affected individuals, eroding trust in the healthcare system's ability to protect their sensitive information and could result in legal consequences and penalties. To mitigate these risks, healthcare organizations must prioritize robust cybersecurity measures, including regular training for staff on best practices for cybersecurity, implementing advanced threat detection systems, maintaining up-to-date security protocols, and conducting thorough risk assessments. Additionally, a well-defined incident response plan can help organizations to respond effectively in the event of a security breach.

In another scenario, we consider **a pandemic like COVID-19 disrupts the digital sector**, leading to workforce challenges (as the digital sector heavily relies on a skilled workforce), increased demand of digital services (including remote collaboration tools, online education, and e-commerce), intensified cybersecurity threats caused by rapid digital transformation and many others. To address these challenges, authorities and digital sector operators must prioritize resilience, contingency planning, and the implementation of robust cybersecurity measures. Collaboration between relevant authorities, strategic resource planning, and flexibility in adapting to dynamic situations are the key components to be considered in the scope of this pilot.

This pilot involves collaborative efforts of **2 national and sectorial authorities and 2 CI operators**, namely the Romanian Ministry of Health (**MoH**) – the National Authority for Health sector, **DNSC** – the National Authority for Cybersecurity, Dr. Muntean Clinic (**CGDM**) – one of the health operators in the private sector, and the General Directorate for Internal Protection (**DGPI**) – part of the Ministry of internal affairs that operates the digital infrastructure and essential services such as authentication of citizens in the online environment in order to access electronic public services of central and local public administration, as well as commercial services provided by the private sector that require the online authentication of personal identity.

1.2.3.4. MICRO Pilot ITALY [led by INS in T9.4&T10.4]

The lessons learned from COVID-19 pandemic show how **service digitalization plays a key role in future of Public Administration** (PA). Fostering the offer of digital public services and accelerating the implementation of key e-government projects represent strategic digital challenges of Italy's Recovery and Resilience Plan. The path to digital transformation of PAs implies a **re-engineering of their internal processes** in terms of technological innovation, improving their efficiency from quantity and quality point of view. Digital transformation changes, therefore, the role of IT systems and infrastructures in operational continuity of public services; this lead to a change in relevance in the risks that can compromise availability the digital services (e.g., cybersecurity, physical attacks, blackout, etc.). This pilot focuses on **digital vulnerability in the Public Administration in the Friuli Venezia Giulia Region**, which plays a key role in **providing essential services** (e.g., regional healthcare system) and in **managing critical data** about citizens (e.g., personal data, EHR, financial data) and companies. Digital services provided by PA **span multiple sectors** (e.g., healthcare, employment, local taxes, accounting, registry office, social policies, economy, agriculture and food, environmental protection, energy, cartography, tourism, etc.) at **multiple levels** (e.g., regional offices, regional public agencies, municipalities, health companies, hospitals). In case of interruption (caused by a cyberattack or by a physical damage to a fibre cable) of the IT infrastructure, the operational capacity of PA would be compromised; the effects would have repercussions on each stakeholder of digital public services: local PAs, companies and, in particular, citizens. A cyber-attack aimed at the regional healthcare information systems, for example, would cause inconveniences and delays in clinical procedures and examinations, leading disruptions to patients and exposing sensitive data to risk. Other types of interruption of public services could be caused by physical attacks or natural disasters/human-induced disasters involving the ERMES regional high speed fibre network, connecting each local PA. The interruption of connectivity would result in the cascading disruption of PA provided digital and physical services. This pilot is an initiative involving the **Friuli Venezia Giulia Region**, as the entity responsible for the provision of public services, and **INS**, as the provider of ICT services, ERMES, Data Center, information systems, used to implement and deliver such digital services.

1.2.3.5. MICRO Pilot GREECE [led by SYN in T9.5&T10.5]

The MICRO pilot in Greece will focus on the resilience of the enablers of the Public Administration and the (Drinking & Waste) Water Management services. It will focus on the disruptions that stem from **(i)** the heterogeneous distribution of their own resources across different (physical and digital) sites (and **(ii)** the complex networks of (public and private) organizations involved in the supply chains their essential services interface with. Based on experience from recent natural disasters that had a significant impact in the disruption of water supply, the focus of the pilot will be on the development of an integrated flood management methodology for water/wastewater facilities and the **assessment and anticipation of risks regarding the disruption of water distribution** and other impacts to the water-management by EYDAP, due to strong flood events. This pilot will validate strategic level methodologies including forecasting mechanisms for disaster resilience, severity rating protocols and mitigation plans, and comprehensive planning for anti-flood projects. This methodology will undergo implementation as a pilot in a selected EYDAP facility, serving as a testing ground for its effectiveness. The pilot will not only involve the practical application of forecasting tools but will also evaluate the severity rating criteria and the feasibility of anti-flood projects. The insights gained from this pilot initiative will be instrumental in refining the methodology for wider applicability not only in other regions but also in a broader set of potential natural hazards. Following successful implementation in the initial facility, the methodology is poised to be extrapolated to other facilities in Attica. The selection process for future application sites will take into account both operational data from EYDAP and existing flood maps within the Attica Region. Moreover, the methodology will draw from the experiences and findings of related and available recent studies conducted for the Region of Attica, particularly those concerning innovative flood modelling of main streams in Attica Region.

The motivation to engage in ENDURANCE stems from the imperative to fortify water management facilities against the increasing threats of floods, aligning with a broader strategy for resilient urban infrastructure. The involved partners will leverage the integrated flood management methodology as a means to enhance their adaptive capacity, ensuring the sustainable operation of water facilities in the face of evolving climatic patterns and potential flood risks. EYDAP and Region of Attica aim to enhance their flood resilience, minimizing potential disruptions to water supply and facility operations. Additionally, the pilot project will serve as a knowledge-exchange platform, facilitating the sharing of best practices and lessons learned with other water management entities and public authorities. This collaborative approach aligns with the broader goals of ENDURANCE, promoting a collective response to shared challenges. This pilot involves the **Regions of Attica and West Greece**, as the entities responsible for the provision of public services, **EYDAP** as the water/wastewater company in Attica Region, **ICCS** as a research and technology provider with competencies in relevant methodologies and risks analysis and **SYN** as a provider of digital services.

1.2.4. Linked Research and Innovation Activities

The consortium will reuse existing know-how and technologies. Below, we list **relevant past/ongoing projects of which outputs will be used as a baseline for ENDURANCE**, and the partners owning them.

WP	Project	Results (Technology & Experience) to be Reused [Owners]
WP1&2, WP9&10, WP11	HEU SUNRISE, ATLANTIS	SUNRISE Working Group on Pandemic Resilience [**ICS**, **INS**, **TS**, **ELES**, **FVG**]. Organisation of strategic and operational workshops with CI stakeholders, coordination of large-scale pilots with CI authorities and operators [**ICS**, **INS**]. Training material for CI resilience and CI-/CI resilience-focused communication, collaboration, dissemination [**CCL**].
WP3-WP6	HEU LAGO	A Trusted EU Research Data Ecosystem (RDE) to address the lack of domain-specific data and insufficient quality and quantity to enable appropriate development of data-driven and AI-based technologies in the security domain [**ENG**].
WP5-WP10	HEU SUNRISE, ATLANTIS	Risk assessment methodology, methodology for identification of systemic risks in large-scale pilots [**ICS**, **URSIV**]. Risk assessment and decision support platform, intelligence gathering solution [**ENG**, **SYN**].
WP5-WP10	HEU MANOLO, CYCLOPS, DEP CYDERCO	Platforms, frameworks, and technologies for risk identification, threat intelligence sharing, trustworthy data processing (AI), and management of a complete data lifecycle for large-scale volumes of data from heterogeneous sources. [**EVI**]
WP5-WP10	H2020 PLEDGER, H2020 M-Sec	Next-generation IoT, edge, and cloud computing infrastructure, securing stability and effective performance of digital services [**ENG**, **ICCS**].
WP5-WP10	H2020 DEFENDER,	Threat spectrum identification, attack trees for multiple scenarios in CI, interdependence analysis [**ICS**, **ELES**]. Technologies for the protection against large-

	INFRASTRESS, 7SHIELD	scale cyber-physical threats and hazards, and for increasing situational awareness [**ENG**].
WP5-WP10	H2020 PHOENIX, FISHY, GRACE	Blockchain/DLT and federated ML technologies ensuring trusted information exchange [**SYN**, **ENG**]. Technology for increasing cyber resilience of supply chains [**SYN**].
WP5-WP10, WP12	H2020 PRECINCT, CyberSEAS, APPRAISE	Cyber-physical risk assessment methodology, analysis of CI interdependencies and cascading effects [**ICS**, **ENG**, **SYN**, **ELES**, **TS**]. Digital Twin solution [**ENG**]. Legal and ethics analysis [**TLX**].
WP5-WP10	H2020 GEIGER, IRIS, CitySCAPE, SECANT	Know-how on methodologies and technologies for monitoring cyber risks, threat reporting, incident response, awareness raising, and training [**DNSC**, **ENG**].

The maximise the impact beyond the consortium, ENDURANCE will seek synergies with other relevant projects to share results, ideas, and experience. Below, we list **ongoing projects with which ENDURANCE will collaborate**.

WP	Project	Potential Collaboration	Link
WP1, WP2, WP5, WP6, WP9, WP10, WP11	HEU SUNRISE, ATLANTIS	CI cooperation, exchange of know-how on cross-x risk assessment. Joint promotion and impact generation.	ICS, ENG, SYN, INS, CCL
WP1, WP2, WP9, WP10, WP11	HEU EU-CIP	CI cooperation. Joint promotion and impact generation.	ENG

1.2.5. Interdisciplinarity and Integration of Social Sciences and Humanities

ENDURANCE will provide a strategy and technologies for improved resilience of essential services under various known and emerging, natural and man-made threats and hazards. For these results to be effective, it is important they **integrate social norms, account for human factors, and are adapted to the needs of the end-users**.

Previous experiences have demonstrated that ignoring behavioural insights can yield poor (or even counter-productive) results, sometimes putting at risk overall societal resilience. During large-scale and/or long-lasting disruptions in the provision of essential services (e.g., in pandemics, in natural disasters), conflicts arise between the values of life or well-being and various freedoms, and they must be prioritized where they conflict. Therefore, the **social and human aspects must and will be considered throughout the development process**, by design.

To address these challenges, the consortium includes **multidisciplinary expertise** in **strategic CI** oversight (AKOS, URSIV, DNSC, MoH, RDFA, RDFW, FVG), **operational CI** know-how (TS, ELES, DGPI, CGDM, EYDAP, INS), in **security, risk, and business continuity management** (SBT, ICS), and in **research and technology development** (EVI-RO/-DE, ENG, SYN, ICCS). This is complemented by expertise in **Social Sciences and Humanities (SSH)**: ethics and law (TLX), business development (DBC), and communication and collaboration (CCL, ICS).

We are aware of the complexity of communicating combined results from different disciplines. So, we are **involving experts from different disciplines in the different stages of the project**, from the beginning with the analysis of strategic challenges (**WP1&WP2**), across R&D (**WP3-WP8**) and validation (**WP9&WP10**), right to the promotion and exploitation (**WP11**). This approach will allow different members to have the necessary knowledge of what other disciplines offer, thus enhancing communication between disciplines, providing an interdisciplinary perspective based on co-design to address the problems at hand and, ultimately, contributing to rendering ENDURANCE's outcomes future-proof, also, with respect to compliance with forthcoming data- and AI-related EU regulations. Surveys with stakeholders (**WP1&WP2, WP11**) will help to identify current practices and their expectations on new solutions, facilitating the co-design of adapted solutions for end-users. A **research ethics workshop** (**T12.3**) will establish guidelines and principles for anticipating discriminatory uses of data and equip partners with research ethics practices. This interdisciplinary effort will continue in all **WP1-WP10** to introduce specific ethical, legal, and socio-economic requirements tailored to the challenges to be addressed during the design and development of the ENDURANCE strategies and technologies, and to assess the results from the perspective of their own discipline. By involving these disciplines **at all stages**, we ensure that their inputs are considered, all along the process, at the overall approach and individual solution inception, from the design phase, and not as a simple add-on. Finally, **SSH partners will have strong participation** in continuously evaluating multi-disciplinary impacts (economic, societal, and environmental in **T11.5**; ethical and legal in **T12.3**) of ENDURANCE and preparing a roadmap for sustainability of results (**T11.4**).

1.2.6. Gender Dimension

The gender dimension is an important parameter in human interaction, security management, decision-making and, therefore, in CI resilience. Acknowledging, thus, the importance of gender, we will explicitly analyse and consider it in a concrete manner **across several R&D activities** and under concrete outcomes, including by means of a gender policy included in the project handbook (**D12.1**) at an early project stage, in M03, particularly through the following.

Inclusion of a gender perspective in research: Any review of the existing literature, theories, concepts, standards, and legal instruments commonly used in the security area **will identify possible sex/gender differences and/or similarities** for their implications on the outcomes or impact of the project. For instance, women and men often have different roles and responsibilities during crises / significant disruptions, and their specific needs must be understood and addressed. A gender-sensitive approach ensures that the diverse experiences and vulnerabilities of individuals are considered, ultimately enhancing the effectiveness of risk management strategies. By integrating a gender lens into our risk and resilience assessment, we aim to deliver solutions that are attuned to the unique challenges faced by different genders, promoting a more equitable and effective approach to the CI resilience.

Dissemination of results: Relevant gender findings will be targeted at relevant research journals (e.g., Gender & Society). Dissemination materials will be in gender-neutral language.

1.2.7. Open Science Practices

We consider Open Science as an integral part of its innovation approach. This means not only that the results will be made **publicly available and accessible**, as much as possible given the potential security constraints, but also that the **principles of openness, transparency, and democratisation** that ENDURANCE adheres to will be extended to the entire research and innovation cycle of the project.

OPEN ACCESS: Making knowledge freely available to everyone: All partners are committed to make their scientific publications available in open access and all the produced research data publicly available (with full respect to the privacy and fundamental rights). ENDURANCE will publish a minimum of 10+ papers in open access (in, for example, **Zenodo** and/or **arXiv**) and a minimum of 10+ articles in the **Open Research Europe** platform. As further discussed in Section 1.2.8, ENDURANCE also commits to publishing (as openly as possible, as closed as necessary) 5+ datasets to relevant ecosystems (e.g., Common European Data Spaces, national / European) open data platforms.

OPEN SOURCE: Creating openly available platforms, tools, and services: ENDURANCE will ensure that the developed technology (tools, services) will be published **as early as possible** on open repositories (e.g., **GitHub** and the **European Open Science Cloud (EOSC)** portal), with Open APIs that allow interoperability, offering **open-source knowledge** to the scientific community to experiment and to the third-party developers to implement novel applications and avoiding vendor lock-in. As part of the exploitation strategy, the consortium will define appropriate, permissive licenses to maximise reusability of project results without hindering the partners' exploitation paths.

CO-CREATION: Knowledge-creation is more efficient if scientists work together: Through its inclusive and interdisciplinary approach, ENDURANCE will act as a platform for facilitating knowledge exchange in different scientific domains and application areas as it is prominent by the plethora of different partners involved in the R&D activities (**WP1-WP8**), pilots (**WP9&WP10**), and impact assessment (**WP11**). All this knowledge will be coordinated and shared through a common approach, fostering the combination of efforts and collaboration of different stakeholders.

1.2.8. Management of Research Data and Other Research Outputs

ENDURANCE will maximise access to / re-use of the research outcomes, body of knowledge, and datasets generated in **WP1-WP10**. The Data Management Plan (DMP, **D3.1**), which will be continuously updated, will support **FAIR Data Principles**, and will outline the procedures for data storage and protection during and after the project end. Appropriate data repositories will be identified through the OpenAIRE platform, and access restrictions will be defined according to the IPR management strategy (ref. Section 2.2.4, **T11.1**). The DMP will encompass the entire data management life cycle for all datasets and for the retention period agreed therein.

The following data types will be generated and used during the project: **(1) context data**, coming from literature, to set the baseline knowledge for ENDURANCE, **(2) public and private datasets** from end users, open data platforms, and other public sources, and testbed implementations, and **(iii) software components and code**. The table below shows the main research data to be used and generated in ENDURANCE, along their type and expected size.

Any personally identifiable information collected during the project will be **protected and anonymized** according to the GDPR. The consortium partners' **Data Protection Officers** (DPOs) will help to oversee compliance with relevant legislation. A **Project Security Board** [T12.2] will manage security clearance of research data/outcomes.

To enhance **findability** of research outputs, we will adopt persistent and unique identifiers (e.g., DOIs) connected to a set of metadata describing an outcome and/or to the outcome itself. To enhance **interoperability**, the consortium will seek adoption of standard formats and vocabularies for metadata and dataset usage. Licences for data sharing and re-use will be provisioned as part of the IPR management and included in the DMP. We will coordinate datasets curation, storage, preservation (**T3.3 & T4.3**), and will encourage adoption of **permissive data sharing licences**.

WP	Research Data / Outcome	Type	Size
WP1& WP2	Data from discussions and workshops with the CI stakeholders including participants data, discussion notes and minutes.	Text.	80-100 MB
WP3& WP4	Body of knowledge on project-specific requirements, SotA analyses, solution designs, and development and integration roadmaps.	Graphs, text, numerical, UML	200-400 MB
WP3& WP4	Body of knowledge on available CER-relevant datasets (catalogue).	Graphs, text	50-100 MB
WP5& WP6	(**Restricted to CIs**) Registry of defined and identified essential services, critical entities, interdependencies, risks, impacts.	Graphs, text, UML	100-300 MB
WP5-WP10	Algorithms, SW components, ML models, APIs.	Code/executable format	200 MB-2 GB / technology
WP5& WP6	Curriculum and (textual & visual) material for courses on CI resilience.	Graphs, text	~50 GB
WP7-WP10	(**Restricted to project partners**) Various sensory data and data from IT/OT systems relevant for the assessment of risks and resilience (e.g., data from security monitoring systems).	Text, numerical	~10 GB

2. Impact

2.1. Pathways Towards Impact

Our aim is to support the CI authorities and operators in the **implementation of and compliance with the resilience-oriented legislation** (European, national, sectorial). Below, we describe how our results (i.e., Key Exploitable Assets (**KEAs**), Section 2.2.2.2) provide measurable benefits, namely **outcomes** (**OUTx.y**), in the time frame of the project (Section 2.1.1). Here, our **stakeholder community** includes **EU MS authorities and policy makers, CI operators and industry experts, SW engineers and technology developers, researchers, and society**. Afterwards (Section 2.1.2), we elaborate on the **impacts** (**IMPx.y**) that the outcomes (i.e. our **KEAs**) will generate.

For each expected outcome and impact, we present their **scale and significance through KPIs**. For their definition, the following **baselines, assumptions, benchmarks** were considered: **(i)** Consortium size, geographic diversity, and outreach capacity (reflecting the available **channels** to generate impact). **(ii)** Excellence of project results (reflecting the consortium's **means** to generate impact). **(iii)** Current political and socio-economic situation in Europe (reflecting the **needs** that will drive the interest of the stakeholders for the uptake of results).

2.1.1. Contributions Towards the Expected Outcomes

Outcome #1 (OUT1): Tools for EU Member State authorities and operators for the assessment and anticipation of relevant risks to the provisions of essential services are **identified**. ← **KEA1**, **KEA2**

A comprehensive assessment and anticipation of cross-x risks to the provisions of essential services require many different inputs related to **(i)** the functioning of the services as well as the organisations operating, overseeing, and regulating them, **(ii)** their interdependencies, and **(iii)** existing vulnerabilities and all types of relevant hazards and emerging threats. To be able to identify tools that can support the CI authorities and operators in this task, we will first of all facilitate a strong cooperation among them and a **continuous dialogue** with them (**T1.1&T2.1**) to discuss, gather, and analyse the insights on the **current practices, tools, and needs** (**T1.2**, **T2.2**, **T1.3, T2.3**). In parallel, we will analyse the **SotA** (**T3.2, T4.2**) and relevant **data sources** (**T3.3, T4.3**) to identify available means for risk and resilience assessment, and afterwards design (**T3.4, T4.4**) and integrate and deploy (**T3.5, T4.5**) specific tools and components for their realization. Further, we will consider a **wide spectrum of vulnerabilities, threats, hazards, and risks** that stem from the physical and digital environment, as well as from the interdependencies across

the services (T5.1, T6.1). These insights will help to **identify the tools needed and available** for the joint, cross-x risk assessment and anticipation. The results will be included in the CER-relevant Data Space (T5.2&T6.2, KEA2) and the Strategy for Disruption Resilience (T1.4&T2.4, KEA1).

Iterative joint, cross-x stress tests and large-scale exercises (WP9&WP10) will further evaluate tool effectiveness and **identify potential further means** needed for the joint risk assessment and anticipation. Similarly, our engagement, promotion, and business development activities (WP11) will foster open and continuous communication to **gather valuable feedback from the stakeholders** about other available means and tools, about the emerging standards and policies that may shape the tools' relevance in the future, and about the market needs and trends.

Scale & Significance of OUT1: Outcome #1 KpIs				
CIs Engagement Rate	**Key Tool Integration Rate**	**Data Alignment Rate**	**All-Hazard Coverage Rate**	**Tool Usability Rate**
>80% of CI authorities and operators from the Working Group are actively engaged in the dialogue.	**>70%** of the key tools identified in the analysis of current practices and SotA, addressing users' needs, are integrated into the Data Space, Strategy, or Risk & Resilience Assessment service.	**>80%** alignment between the identified data needs and actual data availabilities for a comprehensive, joint risk assessment and anticipation.	**>90%** of all vuln., threats, and hazards identified are integrated into the Risk & Resilience Assessment service and Strategy.	**>75%** level of usability and practical relevance of the ENDURANCE tools and services, as perceived by the users gathered during the workshops, pilots, and promotion.

Outcome #2 (OUT2): The cooperation between authorities of EU MS is facilitated by **providing solutions for data exchange and joint cross-border risk assessments**. ← KEA2, KEA4, KEA5, KEA7

By facilitating strategic cooperation as well as continuous engagement and communication among the competent EU MS authorities (T1.1&T2.1), we will ensure that the developed solutions align with their practical needs and challenges, thereby **influencing and promoting their willingness to engage** in data sharing and joint, cross-x risk assessments.

On a technical level, we will **harmonise definitions and data** relevant for a cross-x risk and resilience assessment (T5.1&T6.1, KEA7), including data on EU MS critical entities, essential services they provide, associated service interdependencies, and relevant hazards, risks, and possible cascading effects. The data will be gathered by and provided to all CI authorities and operators through the **Trusted EU CIR Data Space** (T5.2&T6.2, KEA2) that will provide a trustworthy and standardized environment for the exchange of key information, enabling users to gain a "big picture". Especially in the cross-border contexts, such harmonisation, definition, and data accessibility enhance the understanding of shared risks and vulnerabilities, and thus facilitate strong collaboration in the sense of data sharing and risk assessment that cross national borders. Moreover, by developing and implementing a harmonized data governance structure within the Data Space will ensure that data exchange adheres to common standards and protocols, making it easier for different authorities to collaborate without facing interoperability challenges.

Further, we will **develop specific tools and services for secure data exchange and federated data processing** for cases where data cannot be shared (T7.1&T8.1, KEA4). By developing common protocols, we will address the challenge of the diverse practices and tools used by the EU MS authorities. This **standardization** will simplify the process of sharing sensitive information related to resilience, thus promoting efficient and effective cross-border cooperation.

Finally, we will **deliver methodologies, tools, and services for a cross-x risk and resilience assessment** (T7.2&T8.2, KEA5). These will enable the CI authorities to **collaboratively assess and understand the interdependencies and shared risks**. By providing such a common platform, we directly contribute to the greater cooperation between the EU MS authorities not only in sharing data and assessing risks and resilience, but also in **mitigating risks, effectively managing disruptions**, and fostering a **comprehensive and collective approach to CI resilience**.

Scale & Significance of OUT2: Outcome #2 KPIs			
EU MS Authority Engagement Rate	**Tool & Service Adoption Rate**	**Number of Cross-X Assessments**	**Stakeholder Satisfaction Rate**
>50% of CI authorities from the Working Group contribute	**>10** of CI authorities adopt the developed tools	**>30** of joint cross-x risk and resilience	**>85%** of CI authorities are satisfied with the usability

to the Data Space and data exchange.	and services for risk assessment.	assessments using our solutions.	and effectiveness of our solutions.

Outcome #3 (OUT3): **Simulation tools** are developed for large-scale exercises to test the resilience of operators and of specific sectors, and related **training courses** are designed. ← KEA3, KEA6, KEA7

Our goal is to develop solutions that provide **advanced support to EU MS competent authorities and CI operators** in their collaborative efforts to enhance the resilience of essential services against a spectrum of disruptions arising from cyber, physical, and hybrid threats and hazards. To achieve this, we adopt a multifaceted approach that places the insights from the CI operators and authorities (T1.1&T2.1) at the forefront. By synthesizing these insights with findings from our extensive desk research (T1.2&T2.2, T1.3&T2.3), we will thoroughly analyse the specific operations of critical entities across various sectors. This comprehensive analysis includes understanding of the **cross-x interdependencies** that underscore these essential services and identification of a **wide spectrum of risks** related to cybersecurity, natural disasters, human threats, and technological failures (T5.1&T6.1). In parallel, we will explore the state of the art in simulation tools (T3.2&T4.2) and analyse existing practices in testing and training adopted by CI authorities (T1.1&T2.1, T1.2&T2.2), along with identifying gaps in these practices (T1.3&T2.3). This work will shed a light on the most vulnerable (strategic, technological, and human) aspects of ensuring essential service continuity, and will thereby **provide a great baseline for the need-oriented and user-centric design of simulation tools, joint exercises, and training courses** (KEA7).

Based on the identified needs and gaps, we will synchronously **(i) design simulation and training scenarios** (WP9&WP10) to **rigorously test** operational resilience of CI operators within and across different sectors (focusing on the digital, energy, health, public administration, drinking and wastewater management sectors), leveraging our **cross-x and all-hazard** approach, and **(ii) develop advanced simulation and training tools and services** (including a Digital Twin (T5.3&T6.3, KEA3) and a CI-Range (T7.3&T8.3), KEA6) that implement these scenarios and enable comprehensive, interactive, and large-scale resilience testing in different pilot exercises (WP9&WP10). Throughout, we will evaluate the effectiveness of our solutions using well-defined criteria, ensuring that our tools are both **innovative and impactful**.

Additionally, we recognize the need for robust user engagement, aiming to proactively empower CI stakeholders by offering **tailored material, curricula, and courses** on CI resilience (T5.4&T6.4) along with the training services (T7.3&T8.3, KEA6). This holistic strategy is designed to cultivate a resilient mindset and enable effective responses to disruptions.

Scale & Significance of OUT3: Outcome #3 KPIs		
No. of Stress Tests	**CI Workforce Engagement in Large-Scale Exercises**	**Training Completion Rate**
30+ designs for cross-x, all hazard stress tests.	50+ employees of CI operators from 6+ sectors and 4+ EU MS actively participate in large-scale exercises using the ENDURANCE simulation and training tools.	>50% of users of the Training service complete the training programme.

Outcome #4 (OUT4): **Measures** by MS authorities to facilitate risk assessments by operators are **identified**, including the **assessment of cross-sector** and **cross-border interdependencies**. ← KEA1, KEA2, KEA4, KEA5

One of our key activities is the close **cooperation with the competent authorities** responsible for different sectors in different EU countries – from within the consortium and beyond. In our continuous dialogue with these authorities (T1.1&T2.1), we will gather insights to understand and analyse their current definitions, methodologies, practices, and policies (T1.2&T2.2), as well as their needs and challenges (T1.3&T2.3) in facilitating cross-x risk assessment by CI operators. This collective (and confirmed/validated) understanding of the existing landscape will enable us to **propose harmonized definitions, methodologies, and procedures** for the cross-x risk and resilience assessment, as well as for the joint and effective disruption preparedness and response. These results will be gathered in the **Strategy for Disruption Resilience** (T1.4&T2.4, KEA1), which will be continuously validated and improved (T1.1&T2.1, WP9&WP10).

This work will also be fed by our **(i) analysis of the cross-x interdependencies**, and **(ii) identification of the wide spectrum of threats and hazards** arising from the cyber, physical, human domains, as well as from the previously identified cross-x interdependencies (T5.1&T6.1).

To solidify these efforts, we will **(i)** establish a Trusted EU CIR Data Space (T5.2&T6.2, KEA2) to **ensure availability of key information** for cross-x risk assessment, and **(ii)** implement secure data exchange technologies (T7.1&T8.1, KEA4) and cross-x risk assessment services (T7.2&T8.2, KEA5) to empower

the EU MS authorities to facilitate and practically **enhance the cross-x risk assessment capabilities** of the CI operators with a **cohesive and unified approach**.

Scale & Significance of OUT4: Outcome #4 KPIs		
Strategy Dialogue Rate	**Strategy Validation Rate**	**Strategy Alignment Rate**
>80% of the CI authorities from the Working Group are actively engaged in the dialogue.	**>50%** of the CI authorities from the Working Group are actively engaged in the validation of the ENDURANCE Strategy.	**>30%** of CI authorities from the Working Group align their practices with the ENDURANCE Strategy during the project.

Outcome #5 (OUT5): Provide common European guidance and support for the drafting of their **resilience plans** to meet all the provisions of the proposed CER-Directive: risk analysis, domino effects, cross-sector and cross-border analysis, standardised plans, educational and training tools. ← **All KEAs**

We **actively guide and support the CI stakeholders** in their understanding of / compliance with the CER-Directive by **(i)** gathering the knowledge, sharing the CER-relevant data, and **developing tools and services** for the cross-x risk and resilience assessment (**WP5**, **WP6**, **WP7**, **WP8**, **KEA2**-**KEA7**), **(ii) harmonising** the definitions, methodologies, and approaches across EU for enhancing resilience, thereby enabling a **unified and standardised drafting of business continuity / resilience plans** (**T1.4&T2.4**, **KEA1**), **(iii)** delivering user-centric materials, courses, tools, and services for **resilience-oriented education and training** (**T5.3&T6.3**, **T5.4&T6.4**, **T7.3&T8.3**, **KEA6**), and **(iv)** continuously validating our results and **directly guiding the CI stakeholders** in meeting the provisions of the CER-Directive through the national and European workshops (**T1.1&T2.1**) and through the joint, large-scale exercises with the CI operators and authorities (**WP9&WP10**).

Through the ENDURANCE framework and, specifically, through the user-centric advanced dashboards (**T7.4&T8.4**), the EU MS authorities and CI operators will be able to access CER-relevant data, tools, and services that **(i)** enhance **communication and collaboration** across organisations, sectors, and countries, **(ii)** enable secure and continuous **sharing of guidelines and best practices**, and (iii) provide support in **drafting their own resilience plans**.

Scale & Significance of OUT5: Outcome #5 KPIs	
Strategy Satisfaction Rate	**Resilience Plan Alignment Rate**
>90% of the CI authorities and operators from the Working Group positively evaluate the Strategy on Disruption Resilience.	**>30%** of CI operators from the Working Group align their resilience plans with the Strategy during the project.

Outcome #6 (OUT6): An **all-hazards framework** is created to support MSs in ensuring improved concepts and instruments for the anticipation of risks to entities providing essential services, resulting in an improved preparedness & response against disruptions of key sectors in the EU and enhanced resilience of the EU market. ← **All KEAs**

With the setup of the **Working Group on Disruption Resilience** (**T1.1&T2.1**), we are establishing and fostering a dynamic environment for strategic cooperation among EU MS authorities, laying the groundwork for a unified European approach to resilience. Our commitment extends to providing more than just a cooperation environment; we are **providing a European Strategy for Disruption Resilience** (**T1.4&T2.4**, **KEA1**) encompassing **harmonized definitions, methodologies, and guidelines**, aligning with the provisions of the CER Directive and facilitating a collective front against disruptions. Further, we aim not just to meet the provisions of the CER Directive but to **surpass them**. We're building a resilient foundation that embraces diversity, complexity, and the evolving nature of risks. Our strategy is not a static document; **it's a living, adaptive framework** that reflects the dynamic challenges faced by CIs.

Moreover, we are not merely focusing on theoretical constructs. We are creating practical solutions—a CER-relevant data space coupled with a suite of tools and services (**WP5**, **WP6**, **WP7**, **WP8**, **KEA2**-**KEA6**) for joint anticipation and assessment of risks. Our approach to their design and development is rooted in an **all-hazard perspective** (**T5.1&T6.1**) that goes **beyond singular threats**, embracing the complexity of interdependencies across sectors and countries.

Our vision spans a **wide spectrum of threats, hazards, and risks**, recognizing the diversity of challenges faced by the CI operators in **(i) human-caused threats** like sabotage, cyber-attacks, and conflicts, **(ii) technological hazards** including industrial accidents and infrastructure failures, **(iii) natural disasters** such as floods, earthquakes, and wildfires, **(iv) environmental issues** like water pollution, climate change, and geomagnetic storms, and **(v) health emergencies**, encompassing, among others, pandemics, waterborne illnesses, and biological terrorism (**KEA7**).

Scale & Significance of OUT6: Outcome #6 KPIs		
Strategy Adoption Rate	**Tool and Service Adoption Rate**	**All-Hazard Implementation Rate**
>30% of CI authorities from the Working Group adopt the Strategy during the project.	**>30%** of CI operators and authorities from the Working Group adopt the ENDURANCE tools and services during the project.	**>90%** of all identified threats and hazards are actively integrated into the risk and resilience assessment service.

2.1.2. Contributions Towards the Expected Wider Impacts

Impact #1 (IMP1): Ensured **resilience of large-scale interconnected systems infrastructures** and the entities that operate them in in case of complex attacks, pandemics, natural/human-made disasters, impacts of climate change. ← **All KEAs**

Every chain is as strong as its weakest link. In the context of large-scale interconnected infrastructures and services they support, the weakest links are individual critical entities operating individual services within single sectors and countries. Our approach in the development of the tools, services, and strategy **addresses challenges of / provides support to individual entities** (e.g., energy provider), **services** they provide (e.g., electricity distribution, grid maintenance), **sectors** they belong to (e.g., energy, digital), and **countries** they reside in (e.g., Slovenia, Romania), but, most importantly, our approach **enhances resilience of the interlinked, intertwined, transboundary, large-scale European network** of entities, infrastructures, and services. This is reflected in our plan to **enhance cooperation** among/with different CI stakeholders (**T1.1&T2.1**), prepare a **harmonised, European strategy** for disruption resilience (**T1.4&T2.4**, **KEA1**), develop tools and services for **collaborative, cross-x risk and resilience assessment** and training (**WP3-WP8**, **KEA1**-**KEA6**), and coordinate **joint, cross-x, large-scale exercises** (**WP9&WP10**, **KEA7**).

In our work, we consider **different types of interdependencies**, including **physical** and **geographic** (e.g., shared facilities or facilities in close proximity), **digital** (e.g., integrated IT networks), **supply chain-related** (e.g., having common suppliers), **cross-sectorial** (e.g., one service is essential for the operation of another), etc. As elaborated in our contribution to **OUT6** above, in cooperation with CI authorities and operators, we consider a **wide spectrum of complex threats, hazards, and risks** arising from the environment, nature, health, technology, and humans (**T5.1&T6.1**).

Scale & Significance of IMP1: Impact #1 KPIs				
Interdependency Awareness Index	**All-Hazard Risk Awareness Index**	**Disruption Preparedness Index**	**Compliance Cost-Effectiveness Rate**	**Service Availability Improvement Rate**
>70% greater awareness of cross-x interdependencies among the CI employees.	**>70%** greater awareness of complex threats, hazards, and risks among the CI employees.	**>50%** greater preparedness to large-scale disruptions among the CI employees.	**>30%** greater cost-effectiveness in compliance to resilience-oriented legislation (CER, NIS2).	**>10%** improvement in resilience / availability of essential services, on average per entity.

Impact #2 (IMP2): Upgraded systems for **resilience of the operators** and the protection of CI to enable rapid, effective, safe, and secure response and **without substantial human intervention** to complex threats and challenges, and better assess risks ensuring resilience and open strategic autonomy of European infrastructures. ← **KEA2**-**KEA6**

All our tools and services are designed in a way that increases level of automation in response to complex threats and challenges without the need for a substantial human intervention: **(i)** The trusted data space (**T5.2&T6.2**, **KEA2**) and services for secure exchange and federated processing of information (**T7.1&T8.1**, **KEA4**) provide seamless and secure access to high-quality CER-relevant data **without the need for manual collection or pre-processing, or for human supervision**. **(ii)** The services for multi-dimensional risk and resilience assessment (**T7.2, T8.2**, **KEA3**, **KEA5**) include data/AI-driven technologies that assist CI operators and authorities in maintaining situational awareness, making evidence-based decisions, and effectively preventing or responding to disruptions, thus **reducing the need for manual (possibly error-prone) assessments**. **(iii)** Our simulation and training tools provide comprehensive visualisations and immersive experiences to facilitate realistic and data-driven training scenarios for operators (**T5.3**, **T6.3**, **T5.4**, **T6.4**, **KEA6**). These tools harness advanced technologies such as digital twins and CI-ranges that mimic real-world disruptions and thereby provide the operators means for **hands-on, practical, and cost-effective exposure to complex threats in a simulated environment**.

Scale & Significance of IMP2: Impact #2 KPIs				
Data Management Efficiency Rate	**Cross-X Risk Assessment Effectiveness Rate**	**Decision-Making Accuracy Rate**	**Training Cost-Effectiveness Rate**	**User Satisfaction & Confidence Rate**
>80% reduction in the time required to access and process CER-relevant data.	**>80%** reduction in the time required for cross-x risk assessment.	**>75%** accuracy in decision-making by CI operators in mitigating risks of disruptions.	**>30%** greater cost-effectiveness in personnel training.	**>85%** user satisfaction and confidence when using our training tools and services.

Impact #3 (IMP3): **Resilient and secure smart cities** are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity. ← KEA1, KEA7

The consortium includes representatives of public administrations and regions (FVG, RDFA, RDFW) as well as local/regional CI operators of CI (e.g., regional digital service provider INS, private hospital CGDM) that are a **link with smart cities**. Our results will thus also **incorporate challenges that are inherent to the complex systems** in smart cities and will also be **based on the needs of smart cities**.

The developed solutions, know-how (KEA7), and strategy (KEA1) will be, through these links, **disseminated to other actors in the smart city domain**. Through all the participating CI operators and authorities, large companies and SMEs, and research organisations, we will be able to reach, support, and **influence a wide audience of different smart city stakeholders** (governments, start-ups, industry, citizens, planner, architects, etc.) across Europe.

Scale & Significance of IMP3: Impact #3 KPIs		
Smart City Stakeholder Engagement Rate	**Smart City Reach Index**	**Smart City Satisfaction Rate**
>10% of Working Group members will be representatives of smart cities across Europe.	**20+** of European smart cities/ / smart city regions are directly influenced by the project in terms of resilience enhancement.	**>85%** of smart city representatives are satisfied with how the Strategy addresses the challenges and needs of smart cities.

2.1.3. Requirements and Potential Barriers

We have investigated requirements and potential barriers that may hinder the achievement of the envisioned impact. ENDURANCE will strive to **use the potential barriers and requirements as enablers to unleash its potential**.

Potential Barriers	Mitigation Measures
Sustainability: The adoption of new tools, services, and working models requires investments and adequate funding.	**Demonstration of benefits**: The demonstrated increased ability to anticipate risks [**WP5-WP8**], clear optimisation of efforts in risk management [**WP7-WP10**], and the overall reduction in negative impacts (social and economic-financial) [**WP11**] brought to the end users by ENDURANCE will influence future investments.
Alignment with other initiatives: Ensuring alignment and complementarity with other efforts working on the CI resilience (e.g., the CEGR Expert Group) is crucial.	**Collaboration with other initiatives**: We will actively seek collaboration [**WP1&WP2**] with related initiatives (including other EU-funded projects working in this area) to foster synergies, avoid duplication, and enhance the overall impact of CI resilience efforts across the EU.
Resistance to change: There may be resistance to changes in processes, technologies, and organizational structures, which can make integration more difficult.	**Co-creation**: Engagement of stakeholders in cooperation [**WP1&WP2**], needs and requirements definition [**WP3&WP4**], joint exercises / pilots [**WP9&WP10**], and the exploitation [**WP11**] stages of the project would guarantee a significant adoption of the proposed solutions.
Lack of capability: Some organisations lack the necessary capability to change the risk assessment and/or management.	**Training & awareness**: The involvement of stakeholders in community building [**WP1&WP2**] and joint exercises incl. training [**WP9&WP10**] will raise awareness, develop skills, and support the definition of change paths aimed at modifying / improving the capability to adopt new approaches to risk management.
Regulations & standards: Changes in standards and laws on CI resilience and digital technologies	**Continuous monitoring**: We will regularly monitor regulatory landscapes [**T12.3**], technological trends [**T3.2&T4.2**], and

could impact the relevance and compliance of our solutions.	market dynamics [**T11.4**] to proactively identify changes that may impact the project.
Market dynamics: Shifting market demands, emergent technologies, or alterations in user preferences could affect the reception and applicability of our solutions.	**Stakeholder engagement**: We will establish ongoing dialogues with the end-users / CI stakeholders to understand evolving needs, thereby ensuring that the project remains aligned with user expectations.
Technology evolution: Rapid advancements in technology beyond the project end may necessitate adaptability to ensure our solutions remain cutting-edge.	**Adaptive development:** We will design our solutions with flexibility to accommodate emerging technologies and evolving regulatory requirements to maintain relevance over time [**T3.4&T4.4**].
User behaviour and adoption: The acceptance and adoption of our solutions may be influenced by factors such as user behaviour, organizational culture, or competing priorities.	**User-centric design**: We will employ user-centric design principles to ensure that solutions resonate with the end-users and are more likely to be adopted as user behaviour evolves.

Requirements	Mitigation Measures
Data governance: Effective data governance is crucial for maintaining data integrity, ensuring compliance, and managing data lifecycle.	**Robust data governance framework**: We will implement a robust data governance framework that includes clear policies, procedures, and responsibilities for managing data quality, security, and compliance [**T3.3&T4.3**].
Data privacy: Protection of personal / sensitive data must be ensured when collecting, processing, storing data.	**Privacy by design**: Data protection, anonymization, and privacy-aware processing [**T7.1&T8.1**] will be integral part of the project.
Security: Given the sensitive nature of data, it is crucial to meet stringent security requirements to protect against unauthorized access, breaches, and other cyber threats.	**Security by design**: We will adopt secure data handling practices, including encryption, access controls, and regular penetration tests, to address the specific security requirements [**T3.5&T4.5**, **WP9&WP10**].
Interoperability: We need to ensure that data from different sources, sectors, and countries can seamlessly interact and be integrated.	**Standards development**: We will participate in and/or advocate for the development of interoperability standards [**T11.3**] that facilitate seamless data exchange across different systems.
Scalability: Over time, there might be an increased demand for more extensive datasets. We need to ensure that the data infrastructure can scale effectively to meet growing needs.	**Scalable architecture**: We will design [**T3.4&T4.4**] and deploy [**T5.2&T6.2**, **T3.5&T4.5**, **WP9&WP10**] a scalable data architecture that can accommodate growing data needs without compromising performance.
Data access and sharing: Different stakeholders might have varying requirements regarding access to / sharing of data. Establishing clear protocols and mechanisms is essential.	**Collaborative protocols**: We will establish collaborative protocols and agreements for data access and sharing [**WP1**, **WP2, WP3, WP4**], thus covering the interests of various stakeholders.

2.2. Measures to Maximise Impact

2.2.1. Dissemination, Standardisation, and Policy Making

The ENDURANCE dissemination strategy will ensure that the project results are widely shared with appropriate target audiences, at appropriate times, and through appropriate channels. The project is aligned with technology, policy and societal trends and has the potential to impact the market shortly after the project ends. The positive momentum that will be generated through the pilots will be further scaled across Europe. Synergies between EU-funded actions in the resilient CI domain will be increased through continuous clustering. The dissemination strategy (see below) is based on the cornerstones of effective and impactful communications, the **5 Ws** and an **H**; **what** is disseminated and **why**, **who** are the target audiences, **where**, **when**, **how** are the dissemination activities undertaken.

Why: It is crucial to promote the project and its results to external stakeholders to ensure that: **(i)** the project outputs will be brought to market and fully exploited, facilitating their scale-up; **(ii)** the knowledge gained through the project can be made available to all interested individuals and organisations, and reused in the future; **(iii)** the project reaches decision-makers to contribute to the strengthening of Europe's critical entities.

What: The vision, objectives, strategic relevance, progress, highlights, results, technology, open research data, collaboration networks, impacts, best practices, lessons learned.

Who: **Key target audiences** include **EU MS competent authorities and CI operators** in all critical sectors (primarily focused on energy, digital, health, drinking water, waste water and public administration),

in both the public and private sphere and at the strategic and operational level; the ICT and security **research community** incl. higher education & research, related R&I projects and clusters, in particular the European Cluster for Securing CI (ECSCI) and the Community for European Research and Innovation for Security (CERIS), other relevant CL3 projects; **innovators and ICT service providers** including technology developers and solution providers; Digital Innovation Hubs, experts in cyber/IT security and critical infrastructure, legal and ethical experts, CISOs, CIOs, CSIRTs, CSOs; **Enablers and facilitators:** European and national **policy makers** in CI protection, the Critical Entities Resilience Group (CERG), the NIS-2 Cooperation Group, EU bodies incl. European Commission DG CONNECT and DG HOME; ministries of the interior and of business & innovation, national health authorities; infrastructure, and economy, data privacy **regulators**, **standardisation** bodies and standardisation authorities, national communities of users on disaster resilience; European Reference Network for CI Protection (ERNCIP); South-East Europe Corporate Security Association; Slovenian Corporate Security association.

Where: *** Dissemination channels:** top-level scientific publications, conferences, workshops and webinars, EU networks and resources; university lectures, courses, and seminars, blogs, podcasts, media outlets such as The Conversation; open access through Zenodo/Open Research Europe, EC services such as Horizon Results Booster, Horizon Results Platform and Innovation radar, partner newsletters. * **Scientific journals:** IJCP Int. Journal of CI Protection; IJCIS Int. Journal of CIs; Health, Risk & Society; IEEE Transactions on Dependable and Secure Computing/ Network and Service Management / Information Forensics and Security / Power Delivery; Future Generation Computing Systems; EPJ Data Science; ACM TOPS. * **Scientific conferences:** CRITIS, CIPRE-expo, CS4CA, IFIP WG11.10, ESREL, ISCRAM, IEEE ICDM, ICDE, ESORICS, ARES; Annual Spanish PIC congress (CI Protection); Nicosia Risk Forum; Int. Conf. Days of Corporate Security (ICS); Other: CERIS events, eDelivery events, European Researchers' Night, IT events such as NTK (SI), events relevant to the pilot domains.

When: Measurable (SMART) targets will be set and progress towards them will be measured and evaluated continuously. ***** **Y1**: Development of project brand and identity, website launch (by M03), awareness raising, dissemination and communication strategy development (by M06), early implementation (by M12). * **Y2**: Core impact building activities, engagement, networking, knowledge transfer (M13-M24). * **Y3** and beyond: Results-focused dissemination activities, post-project impact creation (M25-M36).

Post-project sustainability: Dissemination channels will stay live for 5 years after the end of the project. Matchmaking with investors and related projects will take place via the Horizon Results Platform. Expressions of interest to commercialise solutions will be submitted to Horizon Results Booster.

When: **Dissemination mechanisms and KPIs: * Scientific excellence**: Publications in high-rank open-access journals (10+); articles uploaded to the Open Research Europe platform (10+), datasets uploaded to relevant open access platforms (10+), workshop presentations (10+); university theses on ENDURANCE topics (4 MSc, 1 PhD); Papers citing ENDURANCE research (50). * **Awareness raising and dissemination through events**: Participation in conferences (20), trade fairs/exhibitions (15); workshops/seminars (2/year); organisation of local workshops in pilot countries rounds 1-3; European workshop rounds 1-3, organisation of a public final event. * **Networking, clustering and knowledge transfer**: Meetings with relevant projects/initiatives at national/EU level (10); joint technical/dissemination workshops (3); training sessions (10), white paper (1), policy briefs (2), policy webinar (1). These initiatives serve as powfor al fora for extensive knowledge transfer and vital interaction with experts in the field. Thanks to the ENDURANCE consortium members' significant prior involvement in the ECSCI cluster and CERIS, the project will seamlessly deepen the collaboration and strengthen the pre-existing links with relevant actors with regards to research, technical, ethical and societal aspects.

Standardisation and policy making: Market acceptance of the ENDURANCE innovations will be accelerated by building on and promoting relevant existing (EN 17483-1:2021) and emerging **standards in the CI resilience**. EN 17483-1 provides the general foundation of a complete standards system for critical infrastructure protection (CIP). ENDURANCE will contribute to the development of future sector-specific standards in selected pilot domains: energy, digital, health, drinking water, waste water and public administration. Standardisation plays a key role in supporting the implementation of the regulatory framework (CER and NIS2 Directives) to ensure quality in organisation, processes, personnel, and management when delivering services in CIP. Through the pilots, the project will provide evidence-based insights that will proactively identify and mitigate the vulnerabilities of critical entities across the EU. To help turn strategy into action, the project will also draw on prior policy work on the resilience of CIs, e.g., by the EU, the WHO and the OECD and key actors listed under stakeholder groups above. Key channels for policy making will include the ENDURANCE white paper, policy briefs and policy webinar on the tools

for strengthening Europe's critical entities. The CI authorities in the consortium (SI, RO, IT, EL) will facilitate the feeding of results into the work of relevant EC expert groups. The consortium will engage with the community to co-create a roadmap with policy recommendations that will support standardised plans for the CER management and implementation of the associated directives. With the support of the consortium SSH experts, we will support the relevant EU policy actions on AI, ensuring that the solutions developed are socially robust and ethically sound.

2.2.2. Exploitation Plan and Sustainability Pathway

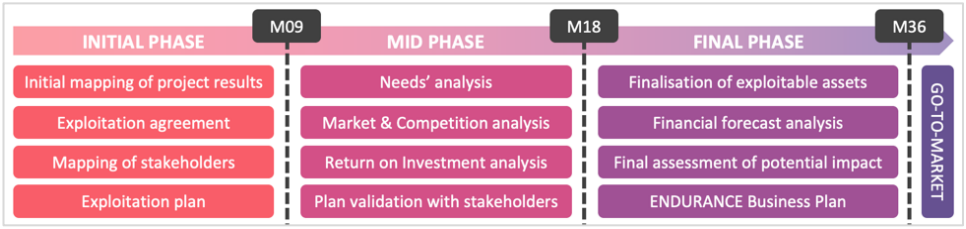
One of the major activities involved in ENDURANCE is the **exploitation of the expected outcomes**. As a result, in close coordination with our dissemination strategy and activities, we will follow an effective, concrete and dynamic exploitation strategy that will be regularly reviewed and expanded as the project proceeds and new opportunities or obstacles arise. To this end, an ENDURANCE exploitation team will be formed to deal with succession and long-term exploitation and continuation issues that arise, with a view to secure the sustainability of the project's services and dissemination scheme. **All partners will nominate qualified persons as exploitation managers** to coordinate the relative activities and scheme. The exploitation team will continuously try to use the stakeholders' community (within and outside the consortium), and all foreseen events and engagement activities to promote the project within an active network aiming at establishing strong working relationships with key people and organisations involved in or having an interest in ENDURANCE domain of relevance. The exploitation activities will be thoroughly planned as the project unfolds and reveals its value and will continue throughout the entire lifecycle of the project.

There is a dedicated tasks for exploitation and future sustainability (**T11.4**), working hand-in-hand with technical and validation work packages (**WP1**-**WP5**), highlighting the importance of this dimension in a **Go-To-Market-oriented approach**. During the project, a set of specific actions will be undertaken to support effective exploitation of project results and outcomes working towards sustainability and impact. In particular:

- [M01-M06] An **Exploitation Plan**, for market exploitation of the results will be defined, detailing exploitation strategy, return on investment analysis, and main actions during and after the project (serving as a blueprint for a **Sustainability Plan**). This will include **Business Plans** building on the initial approach presented below.
- [M01-M06] A joint **Exploitation Agreement** (complementing the Consortium Agreement) among the project partners will be prepared (and signed in the final stages of the project) to ease joint and individual exploitation. It will include the identification of IPR and roles across different exploitation channels.
- [M12-M36] Specific **market impact and business model analyses** will be done to define market opportunities, stakeholders, and potential value chain development. From a preliminary analysis, the markets addressed by ENDURANCE will be CI (resilience) and security (including cybersecurity). Detailed analyses of these markets and most relevant segments will be carried out continuously to ensure successful go-to-market for project results. This will not only validate our innovations but also pave a market-oriented pathway for potential clients, thus fostering sustained societal benefits beyond the end of the project.
- [M12-M36] A **Return on Investment (RoI)-based exploitation analysis** to expected return by target users adopting the ENDURANCE results will be done, including a comprehensive return assessment (not exclusively monetary) taking into account aspects such as increased employees' and citizens' safety, social/economic costs etc. The analysis will help validate the project results from a business/impact point of view and shape value propositions, business plans, and sustainability strategy.
- [M06-M36] **Internal exploitation meetings** and **Exploitation Workshop** will be held during the project. This will enable all partners to fine-tune exploitation strategy and vision as well as to agree upon the IPR strategy.
- [M01-M36] Involvement of relevant **external stakeholders** in the exploitation through tailored activities initiated also to exploit the piloting activities and link to active users, as well as potential customers created through the community. This step will be important to validate the exploitation plan with real 'potential clients', secondly to gather insight from external experts tailored to the project domain. It also positions ENDURANCE pilots not only as a validating activity, but also as a market-oriented step for potential customers.
- [M01-M36] **Potential impact** of our solutions on the critical sectors and the more general public security/safety domains will be assessed. The analysis will be performed based on the KPIs at

objective and pilot levels. The results of this analysis will feed the exploitation strategy by understanding which CIs would be more permeable to the proposed innovations.

Exploitation activities will **start early** and follow an exploitation path throughout the project duration. They will be organised in **3 phases**, as shown on the right, with the exploitation milestones in the various phases. This approach will ensure a **smooth Go-to-Market beyond the end of the project**.



2.2.2.1. SWOT Analysis and Preliminary Business Plan

The **initial SWOT** analysis for ENDURANCE solutions is shown below.

Strengths	Weaknesses	Opportunities	Threats
• We emphasize COOPERATION AT ALL LEVELS, fostering active engagement of CI authorities, operators, and other stakeholders. • We address the interconnections of essential SERVICES, going beyond the siloed focus on critical assets, and we take an ALL-HAZARD approach to assessing risks and resilience. • We deliver pragmatic solutions for enhancing CI resilience, built in a CO-CREATIVE way with the CIs from ALL EU MSs and sectors. • Our solutions directly support the CI authorities and operators in the IMPLEMENTATION OF / COMPLIANCE WITH the CER Directive. • Our solutions will be validated in cross-x LARGE-SCALE EXERCISES with CIs across the EU. • We provide comprehensive TRAINING materials and services empowering CI employees in effectively managing disruptions.	• The CI authorities and/or the operators may not be particularly interested in SOPHISTICATED ICT solutions, especially in economic crises. • The ENGAGEMENT of CI authorities from all EU MSs and CI operators from all critical sectors, and an effective management of the Working Group and its events is challenging. • The DEVELOPMENT of innovative, data-driven solutions is complex, time-consuming, and costly. • The end users may be reluctant to share sensitive DATA for a joint, cross-x risk assessment despite the use of advanced privacy-enabling and security-ensuring approaches and technologies.	• CI authorities and operators have a real NEED for harmonizing approaches, data, and technologies for a joint management of risks and resilience. • Successful adoption of our results is REPLICABLE across all EU countries and critical sectors. • We are taking a USER-DRIVEN approach, enabling the identification of concrete strategic and operational challenges, ensuring solutions meet user and market needs. • Our innovative technologies can generate new KNOWLEDGE as well as MARKET OPPORTUNITIES on data management, risk assessment, cybersecurity, AI, and more.	• We may face REGULATORY and ETHICAL challenges related to data and AI. • Possible OPPOSITION from those stakeholders who are resistant to change or distrustful of technology. • Very active and COMPETITIVE market in the security (and AI) domain. • HETEROGENEOUS legislation and policies on CI resilience across EU countries and sectors. • DEPENDENCY on AI and (sensitive) DATA requires careful consideration of technical robustness, ethical implications, and alignment with the EU guidelines.

A particular business and marketing plan will be developed including all the major steps for the definition of the strategy to maximize the potential project outcomes take-up after the end of the project. The ENDURANCE strategy to maximise the business impact comprises the following key elements:

- **Results**: Clearly define exploitable outcomes and targeted audiences, differences with other systems, IPRs.
- **Awareness**: Ensure attractiveness of the outcomes and benefits are well-known to all key stakeholders.
- **Validation**: Ensure the solutions developed are validated (pilots) and viable for longer term exploitation.
- **Roadmap**: Develop a project roadmap to 2030, outlining the path for long-term funding and continuation of the ENDURANCE works on the potential for further exploitation of the project results.
- **Exploitation Team**: Define who will be the major actors towards the outcomes' exploitation, their commercialist on interests as well as their business strategies and previous knowledge.
- **Exploitation Maximising**: Ensure that the potential exploiters of the ENDURANCE outcomes are made aware of the support networks, tools, and grants available within the EU and details on how to access them.
- **Risk Assessment**: Provide financial, commercial and production risks.

2.2.2.2. KEAs and Preliminary Business Model Canvas (BMC)

The partners have distinct exploitation interests according to their core activities. New technologies produced in the project will enable **rich joint and individual exploitation opportunities**. Exploitation leads who will coordinate the business development aspects of the Key Exploitable Assets (**KEAs**) with the support of other partners are:

- **KEA1 European Strategy for Disruption Resilience**: **ALL** partners.
- **KEA2 Trusted UE CER Data Space**: **ENG** (lead), EVI-RO/-DE, SYN, SBT, ICCS.
- **KEA3 Digital Twins for Interconnected Essential Services**: **EVI-RO** (lead), EVI-DE, ENG, SYN, ICCS.

- **KEA4 Data Exchange & Federated Processing Services**: **SYN** (lead), EVI-RO/-DE, ENG, SBT, ICCS, ICS.
- **KEA5 Risk & Resilience Assessment Services**: **SBT** (lead), EVI-RO/-DE, ENG, SYN, ICCS, ICS.
  KEA6 Simulation & Training Services: **EVI-RO** (lead), EVI-DE, ENG, SYN, SBT, ICCS.
- **KEA7 Know-how, best practices, recommendations**: **ALL** partners.

With these KEAs, the ENDURANCE industry partners / universities & research organisations / public end users will:

- Enlarge **solutions portfolios**. / Increase **research portfolios**. / Increase **levels of digitalisation & automation**.
- Improve **existing offerings**. / Improve **research results**. / Improve **existing public services**.
- Build **capacity and skills** of workers. / Enhance **knowledge basis** and create new **teaching opportunities**. / **Empower and equip** policy makers and public authority employees.
- Initiate new **business collaborations**. / Enhance participation in **research projects**. / Strengthen **collaboration** within and across sectors (within and across borders).
- Enter new **markets**. / Enter new **scientific communities**. / Form new cross-border/country **collaborations**.

The initial KEA-specific exploitation plans are presented below in the **ENDURANCE Business Model Canvas (BMC)**. It will be regularly assessed, refined, and improved to ensure high impact fast. The final WP11 report (**D11.4**) will include an ownership list and sustainability plans by which all partners will ensure longevity of results.

<table>
<tr><th>Key Partners</th><th>Key Activities</th><th>Value Proposition</th><th>Customer Relationships</th><th>Customer Segments</th></tr>
<tr>
<td>· EU MS CI authorities
· CI operators
· Industry experts
· Policy makers
· Technology developers
· Scientific communities and academics
· Advisors and consultants (legal, ethical, marketing)</td>
<td>· Cooperation with the CI stakeholders
· R&D and integration of our solutions
· Validation (stress tests) with end users (CIs)
· User training
· Knowledge sharing, promotion, business development, networking, recommendations
Key Resources
· Insights from the CI end users and experts
· Data sources and technology infrastructure
· Relevant standards, architectures
· Policies, regulations, and ethics standards
· Researchers, SW engineers, SSH experts
· Initial financial investment</td>
<td>· KEA1: A harmonised approach across the EU for CER Directive implementation and CI resilience
· KEA2, KEA4, KEA5: A comprehensive, joint risk assessment and effective CER implementation / compliance
· KEA3: Increased situational awareness about cross-x interdependencies and risks to essential services
· KEA6: Trained, skilled, aware personnel
· KEA7: Thorougly-tested ideas, best practices, and recommendations for new standards, policies, regulations</td>
<td>· Partnerships with EU MS authorities Ci operators (end users)
· Collaboration with industry experts, SW developers, researchers, SSH (partners)
· Relevant CI resilience communities
· B2B relationships
Customer Channels
· Existing business networks and public-private partnerships
· Special community events, industry events, ENDURANCE workshops
· Marketing campaigns and publications
· Open-source communities</td>
<td>· EU MS CI authorities
· EU MS CI operators
· Technology providers
· Academia and research institutions
· Stakeholders of other complex systems (e.g., smart cities)
· IT/service/consultancy providers
· Investors</td>
</tr>
<tr>
<td colspan="3">Cost Structure
· R&D (personnel), maintenance, new features, consultancy
· Commercial data and IT infrastructure (cloud compute and storage)
· Business development, marketing, sales, legal and ethical compliance fees</td>
<td colspan="2">Revenue Streams
· Revenues generated through SW licences, maintenance, training, upgrades, consultancy
· Dynamic pricing per service per client
· Training and certification program revenues</td>
</tr>
</table>

2.2.3. Communication and Collaboration

The ENDURANCE communication activities will focus on raising awareness among a wide range of non-specialist audiences of the project and the societal, economic, and environmental benefits it generates. The key to ensure mass uptake of the project's results will be to **establish communications partnerships** with pre-existing communities, networks, and associations in the CI domain. The planned communication activities are presented in the table below.

Planned Communication Activities and Targets	
Activity #1: High-quality **communications collateral** including logo, brand guidelines, leaflet, poster, and public presentation made available on our website.	**Target groups:** Related projects, enablers, facilitators.
Measurable Result: Brand guidelines and communications collateral pack including poster, leaflet, infographic, and presentation design with continuous updates, equipped with a QR code leading to the ENDURANCE website. NOTE: *Most of the material will be offered in digital format to limit the environmental footprint.*	
Activity #2: **Dedicated website** with project and case study information, objectives, results, partners, events, contact information, links to other ENDURANCE channels.	**Target groups:** General public interested in societal resilience, ICT and security research community, facilitators.
Measurable Result: Website with continuous updates, biweekly project news updates and at least 10,000 visits by M36. Live for 5 years after the lifetime of the project.	
Activity #3: **Press releases** disseminated to national, European, and international media, including TV, radio, industry magazines and newspapers.	**Target groups:** Media and EC support services as intermediary targets, facilitators, general public.

Measurable Result: 6+ press releases disseminated to EU / national media with 15+ instances of media coverage.	
Activity #4: **Targeted events** incl. conferences, workshops, webinars, training sessions, cluster liaison, and a final event to engage wider stakeholders and foster uptake of the results.	**Target groups:** ICT and security research and tech community, policy makers, CI stakeholders, related projects, industry actors.
Measurable Result: 3 end user community / thematic / innovation workshops, 1 webinar, 10 meetings with related projects (e.g., ECSCI cluster), 10 interview sessions with pilot representatives, participation in 20 conferences, 15 trade fairs/exhibitions; participation in 2 workshops/year, and 1 final ENDURANCE event.	
Activity #5: **Project newsletters** contributing to the CI resilience debate incl. newsletter on ENDURANCE activities, communicated to relevant stakeholders.	**Target groups:** Policy makers; general public, CI stakeholders.
Measurable Result: 6 editions of the newsletter with 200+ readers.	
Activity #6: Active presence on **social media** (Twitter, LinkedIn, YouTube, podcasts) to engage stakeholders with dedicated content.	**Target groups:** General public, related projects, industry, research community.
Measurable Result: 500 Twitter/X followers, 500 LinkedIn followers, 10 videos on YouTube with more than 1,000 views, 1 podcast/audio episode, weekly social media posts.	

The preliminary key messages to be used in our communication activities are briefly presented below.

Selected Key Messages	
Message	**Target Groups**
ENDURANCE **empowers** European CI stakeholders to navigate the complexities of disruption resilience and to implement the CER and NIS2 Directives effectively.	CI authorities and operators.
ENDURANCE delivers **tools and services** that allow CI stakeholders to securely manage data, continuously identify and anticipate threats, and assess risks and resilience in real-time.	Tech/research community.
ENDURANCE provides a **harmonised pan-European Disruption Resilience Strategy** to ensure continuity of essential services and safeguard the well-being of EU communities.	Policy makers

Advisory Board: We will establish an **Advisory Board (AB)** with experts in security, critical infrastructure, law and ethics, standardisation, and policy making who can provide valuable insights, guidance, and feedback on various aspects of the project, and can thus enhance its quality, rigor, and impact. Thematic (remote) workshops will be organised with the AB after key project milestones (in the scope of **T1.1&T2.1** and **T12.1**).

2.2.4. IPR Management

The consortium recognises that management of knowledge and IPR are fundamental for the smooth collaboration among the consortium members the successful exploitation and sustainability of ENDURANCE outcomes during and after the project end. Through knowledge management and the protection of partners' individual interests, we will avoid information bottlenecks related to confidentiality, and thus maximise the chances for elevated market visibility and successful exploitation of the project results. **Management of knowledge and IPR will be integrated within the framework of the Consortium Agreement (CA)**, drawn to be aligned with the policies and context for EC funded projects under HEU and will be further addressed by the IPR Management Plan (included in **D11.2**).

Highlights: For scientific papers, **"green" open access** model will be adopted, making the papers available through the project website and through other repositories (e.g., Zenodo). The protection of the IPR created in the project will be performed through **patent submission**. It will look for opportunities of successfully implementing appropriate creative ideas emerging from the project, with a view on both market and technical aspects.

2.3. Summary

SPECIFIC NEEDS	EXPECTED RESULTS	D & E & C MEASURES
• We need to enhance **cooperation and collaboration at all levels**: among the (national, regional, sectorial) authorities, (public and private) operators, as well as innovators, scientists, and consultants working in the area. • We need to **harmonise** the definitions, methodologies, strategies, guidelines, and policies on resilience across the EU MS to **directly support CIs in compliance** with the resilience-relevant legislation (CER, NIS2). • We need to closely analyse the functioning of the interconnected **essential services** and surpass the sole focus on critical assets. • We need an **all-hazard** approach to assessment of risks that arise from nature, environment, technologies, health, and humans. • We need high-quality data, interoperable tools, and user-friendly services for **joint, cross-x risk and resilience assessment**. • We need stress test scenarios, plans, and technologies for collaborative, **cross-x, large-scale disruption resilience training**.	• Increased cooperation and unity of european CIs with **12 national and 3 European workshops** with **20+** attendees in each, and with a **Working Group on Disruption Resilience** with **100+** members by the end of Y3. • A comprehensive, pragmatic, and harmonised European **Strategy for Disruption Resilience validated** by **30+** EU MS authorities and **60+** CI operators, and then **adopted** by **20+** EU MS authorities. • **Data Space** with EU MS critical entities, essential services, interdependencies, and types of associated threats, hazards, and risks (covering **6+** sectors, **6+** entities, **4+** countries and integrating **10+** data sources). • A set of **TRL7 tools and services** for secure data exchange, cross-x risk and resilience assessment, and joint large-scale training exercises, validated by **13+** CIs in their operational environment. • **30+ stress test designs and execution plans** (covering all identified hazards, sectors, and EU MS) run in **15 cross-x medium-/large-scale exercises**.	**Dissemination, Standardisation, Policy-Making**: • **10+ papers** in high-rank journals and/or industry magazines with **50+ citations**. • **30+ presentations** at industry fairs, scientific events, and/or policy events. • **4 MSc and 1 PhD** theses, **2+ seminars**/year. • **Standardisation** (through, e.g., ISO, CEN). • **Policy making** (through, e.g., Gaia-X, IDSA, ECSCI, CERIS, CERG, NIS2-CG). • **3+ whitepapers** (policy briefs, reports). **Exploitation, Business Development**: A structured **exploitation roadmap** including: • ENDURANCE stakeholders' community. • Stakeholder and market **analysis**. • **3 exploitation workshops**. • Market impact and business model **analysis**. • Cost/benefit and RoI **analysis**. • **Business and sustainability plan** including SWOT, PEST, Five Forces. • **Exploitation agreement** among the project partners for individual / joint exploitation. **Communication, Collaboration**: • **Website** with bi-weekly updates, blogs, news and **10.000+ visits** by M36. • **Social/digital media accounts**: Twitter/X (**500+** followers), LinkedIn (**500+** followers), YouTube (**10** videos with **1.000+** views), **1** podcast / audio episode. • **Media outreach**: **6+** press releases with **15+** instances of media coverage. • **Promotional material**: Continuously updated poster, leaflet, infographics. **6** newsletter editions with **200+** readers.

TARGET GROUPS	OUTCOMES (See Section 2.1.1)	IMPACTS (See Section 2.1.2)
• **7 EU MS authorities and 6 CI operators** (project partners) from **different sectors** (digital, energy, health, public admin., drinking and wastewater management) **across Europe**. • **Other EU MS authorities and CI operators** from the remaining sectors (as defined by CER Directive) and EU countries. • **Operators of security-sensitive or complex infrastructure** (e.g. stadiums, smart cities). • **IT/service/consultancy suppliers** for CIs (within	• Better **strategic cooperation** at all levels across the EU, within and across sectors and countries (measured in the size of the Working Group: 100+ members by M36). • **7 EU MS authorities** (AKOS, URSIV, DNSC, MoH, FVG, RDFA, RDFW) and **>30% of authorities from the Working Group** adopt the **Strategy** by M36. • **6 CI operators** (TS, ELES, DGPI, CGDM, INS, EYDAP) and **>10 other operators** adopt the **Tools and Services** by M36. • **6 CI operators** (TS, ELES, DGPI, CGDM, INS, EYDAP) and **>30% of CI operators from the Working Group** align their **resilience plans** with the Strategy and services by M36.	**Scientific**: • Advancements in the **state of the art** in risk management, security, cybersecurity, data science, computer science, SSH. • Better connection and **cross-fertilisation** between security research and **SSH disciplines** (ethics, law). **Economic**: • **Reduction in time** required for accessing and processing CER-relevant data, and for cross-x risk assessment. • Greater **effectiveness** in personnel training. • Greater **cost-effectiveness in compliance** to resilience legislation (CER, NIS2)

the consortium and beyond). ● **Scientific community** in the field of CI resilience, cybersecurity, security, and data science (within the consortium and beyond).	● 2 research institutes and universities (ICCS, ICS) **improve their research outcomes** by adopting ENDURANCE. ● 7 SMEs and large enterprises (EVI, ENG, SYN, SBT, TLX, DBC, CCL) **enhance their portfolios and market opportunities**.	● Creation of **new market opportunities** in the security, cybersecurity, data science. **Societal**: ● Greater **awareness (>70%)** of cross-x interdependencies and complex risks. ● Better **preparedness (>70%)** to large-scale disruptions. ● Enhanced **resilience and availability** of essential services.

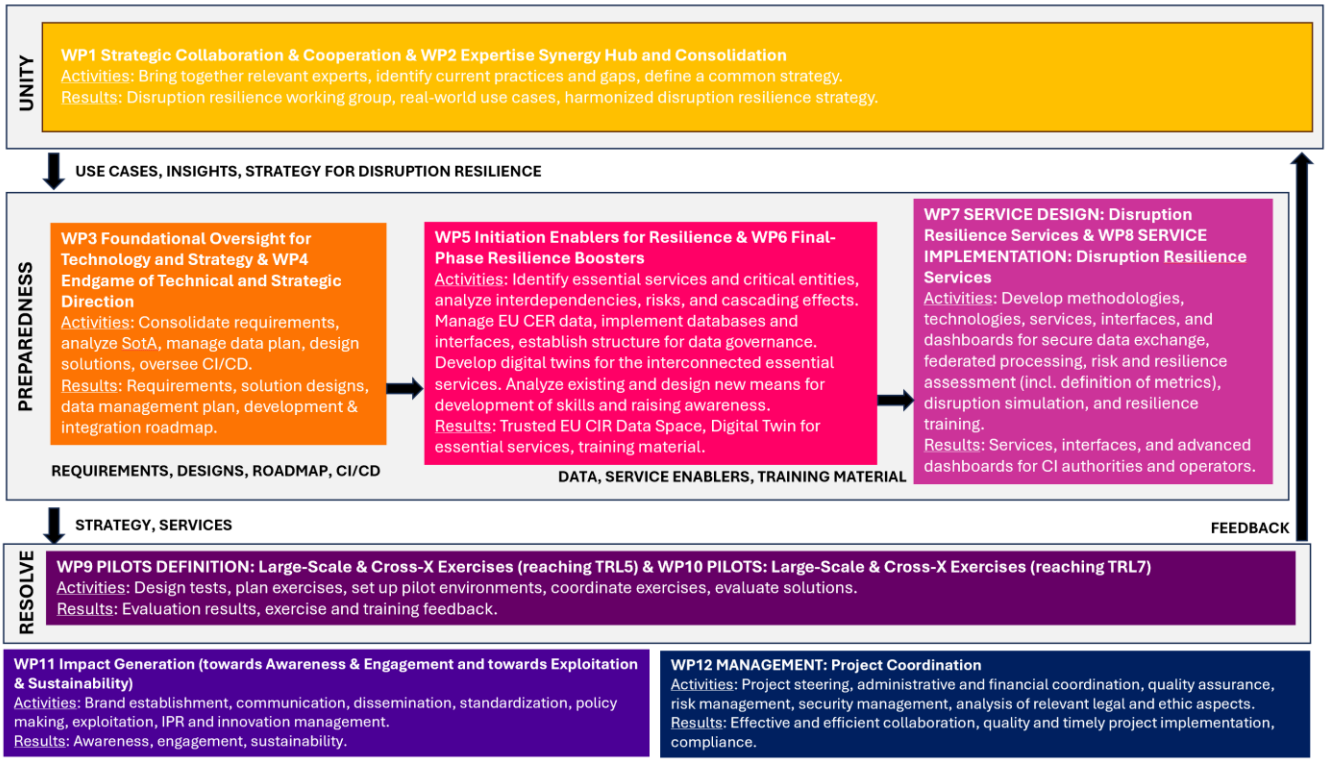
3. Quality and Efficiency of the Implementation

3.1. Work Plan and Resources

3.1.1. Overall Structure of the Work Plan

Project activities are organised in seven complementary Work Packages (WPs), as illustrated below: **WP1&2** is devoted to enhancing strategic cooperation and collaboration among relevant CI authorities, operators, and other stakeholders. **WP3&4** will set up the ENDURANCE concept through a detailed analysis of requirements, design of the solutions, setup of the CI/CD infrastructure, and establishment of the development and integration roadmap. We will **(1)** manage the data and develop the methodologies, technologies, capabilities, and enablers for the ENDURANCE services, and **(2)** develop the services together with the dashboards for authorities and operators in **WP5&6** and **WP7&8**, respectively. The results will be utilised, tested, demonstrated, and evaluated through different joint, large-scale exercises in **WP9&10**.

By adopting an agile innovation approach, the research, development, and validation activities conducted in WP3-WP10 will provide a circular feedback loop to WP1&WP2, thus enabling continuous improvements of the ENDURANCE methodologies, technologies, strategies, and exercises. To achieve the defined impacts, ENDURANCE innovations will be continuously promoted and prepared for exploitation in **WP11**. Project coordination is performed in **WP12**.



To reduce any research, development, or integration risks, we will follow an **agile approach with three overlapping development and integration cycles**, maturing results from **TRL4** to **TRL7**, as illustrated and discussed below.

Path to TRL5 [M01-M18]: We will start with the exploration of existing networks and identification of experts working on the CI resilience topics to be engaged in the **ENDURANCE Working Group** (**T1.1&T2.1**). We will engage members from the consortium and beyond. Then, we will organise several **local / national workshops** (**WL1** by M03) to elaborate country-specific challenges, discuss current practices, and identify opportunities for improvements through concrete use cases. With this information at hand, we will organise a **European workshop** (**WE1** by M06) to identify challenges, practices, and gaps on a European level. We will analyse current strategies and policies for disruption resilience and business continuity plans. The workshops' reports and results of the analysis will be reported at M09 in **D1.1**, which will serve as a baseline for the development of the **ENDURANCE Strategy** (in **T1.4&T2.4**) and **technologies** (in WP3-WP8). The initial **draft of the strategy** will be provided by M15 (**D2.1**), aligning

with the development of the initial service prototypes, and evaluated with CI stakeholders in local workshops (**WL2** at M18).

After the first local workshop at M03, when the use cases and CIs' challenges are refined, we will **start the technical work** (WP3-WP8). First, we will define, consolidate, and prioritize requirements, analyse the SotA, identify available and needed datasets (DMP at M06 as **D3.1**), design the technologies, and establish a development and integration plan, presented at M12 in **D3.2**. In parallel, we will start with the development of the ENDURANCE enabler building blocks (WP5&6) and services (WP7&8), presenting the **initial technological prototypes** at M15 (**D5.1** and **D7.1**).

After the first European workshop at M6, when also the cross-border challenges and goals are refined, we will start designing **small-scale tests for MICRO pilots / large-scale exercises for MESO and MACRO pilots** (presented in **D9.1** at M12) and setting up the necessary environment (e.g., the infrastructure, specific data, protocols, required authorisations, etc.). The initial (lab/local) joint exercises / pilots will be run by M18, testing the designed procedures and basic functionalities of the ENDURANCE services, bringing them to **TRL5**. Results will be presented in **D9.2&D9.3**.

In parallel, we will thoroughly analyse relevant (European, national, sectorial) **legal and ethical frameworks** (**T12.3**) to provide compliance guidelines for the developers of the ENDURANCE Strategy and Services (**D12.2** at M18).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP1: COOPERATION: Strategic Collaboration & Cooperation (Phase 1)			WL1			WE1			D1.1																											
T1.1 Resilience Disruption Networks & Working Groups																																				
T1.2 Resilience Management Definitions & Practices																																				
T1.3 Resilience Management Gaps & Challenges																																				
T1.4 Strategy Definition																																				
WP2: COOPERATION: Strategic Collaboration & Cooperation (Phase 2)															D2.1			WL2			WE2						WL3			WE3		D2.2				
T2.1 Expertise Alliance Enhancement																																				
T2.2 Refinement of Resilience Approach																																				
T2.3 Use Cases Consolidation																																				
T2.4 Enhancement of Harmonised Disruption Resilience Strategy																																				
WP3: ROADMAP: Technical & Strategic Oversight (Phase 1)						D3.1						D3.2																								
T3.1 Definition of Requirements																																				
T3.2 Analysis of the Current State of Affairs																																				
T3.3 Data Needs & Availabilities Definition																																				
T3.4 Design of the ENDURANCE Solutions																																				
T3.5 Integration, Deployment and Roadmap Pathway																																				
WP4: ROADMAP: Technical & Strategic Oversight (Phase 2)																					D4.1											D4.2				
T4.1 Consolidation of Requirements																																				
T4.2 State of Affairs Consolidation																																				
T4.3 Dataset Readiness																																				
T4.4 ENDURANCE Architecture Finetuning																																				
T4.5 Roadmap Calibration & CI/CD Maintenance																																				
WP5: ENABLERS: Disruption Resilience Enablers (Phase 1)															D5.1																					
T5.1 All-Hazard-Oriented Risks & Cross-X Impacts																																				
T5.2 Trusted EU CER Data Space																																				
T5.3 Primary Digital Twins for Interconnected Essential Services																																				
T5.4 Means for Awareness Raising & Skills Development																																				
WP6: ENABLERS: Disruption Resilience Enablers (Phase 2)																																		D6.1		
T6.1 Risks & Cross-X Results Refinement																																				
T6.2 Performance Finetuning for Trusted EU CER Data Space																																				
T6.3 Implementation of Digital Twins for Interconnected Essential Services																																				
T6.4 Awareness & Skill Refinement Capstone																																				
WP7: SERVICES: Disruption Resilience Services (Phase 1)															D7.1																					
T7.1 Architecting Secure Data Exchange & Federated Processing Services																																				
T7.2 Definition of Multi-Dimensional Risk & Resilience Assessment Services																																				
T7.3 Collaborative Large-Scale Simulation & Resilience Training Services																																				
T7.4 Dashboards for CI Authorities & Operators																																				
WP8: SERVICES: Disruption Resilience Services (Phase 2)																																	D8.1 &D8.2			
T8.1 Implementation of Secure Data Exchange & Federated Processing Services																																				
T8.2 Implementation of Multi-Dimensional Risk & Resilience Assessment Services																																				
T8.3 Implementation of Simulators & Training Services																																				
T8.4 Advanced Dashboards for CI Authorities & Operators																																				
WP9: PILOTS: Large-Scale & Cross-X Exercises (Phase 1 - reaching TRL5)												D9.1					D9.2&D9.3																			
T9.1 MACRO Pilot EUROPE: European Cross-X Disruption Resilience																																				
T9.2 MESO Pilot SLOVENIA: Disruption Resilience in Digital & Energy																																				
T9.3 MESO Pilot ROMANIA: Disruption Resilience in Digital & Health																																				
T9.4 MICRO Pilot ITALY: Disruption Resilience in Public Administration																																				
T9.5 MICRO Pilot GREECE: Disruption Resilience in Water Management																																				
WP10: PILOTS: Large-Scale & Cross-X Exercises (Phase 2 - reaching TRL7)																									D10.1&D10.2									D10.3&10.4	
T10.1 Implementation: MACRO Pilot EUROPE																																				
T10.2 Implementation: MESO Pilot SLOVENIA																																				
T10.3 Implementation: MESO Pilot ROMANIA																																				
T10.4 Implementation: MICRO Pilot ITALY																																				
T10.5 Implementation: MICRO Pilot GREECE																																				
WP11: IMPACT: Impact Generation (Phase 1 & Phase 2)			D11.1									D11.2									D11.3														D11.4
T11.1 IPR & Innovation Management																																				
T11.2 Brand & Communication Management																																				
T11.3 Dissemination, Standardisation & Policy Making																																				
T11.4 Define Exploitation & Sustainability																																				
T11.5 Continous Impact Assessment																																				
WP12 MANAGEMENT: Project Coordination			D12.1															D12.2															D12.3				
T12.1 Day-To-Day, Administrative & Financial Coordination																																				
T12.2 Quality Assurance & Risk Management																																				
T12.3 Ethics & Legal Aspects																																				
WP13: Ethics requirements	D13.1											D13.2						D13.3												D13.4						
T13.1 Ethics Aspects																																				
		MS1-START					MS2-CONCEPT			MS3-ROADMAP			MS4-PROTOTYPES			MS5-TRL5			MS6-REFINEMENTS						MS7-TRL6				MS8-STRATEGY					MS9-TRL7	
		Project setup					1st EU workshop			Technical roadmap			Strategy draft			TRL5			2nd workshops						TRL6				3rd workshops					TRL7	
		1st local workshops					Use cases			Stress test designs			Initial data space			Compliance guide			Updated roadmap						Approved strategy, final data space									Fully-fledged services	
		Website, SM					DMP			Impact strategy			Service prototypes			Updated Impact strategy									Reference designs & policy recommendations									Sustainability plan	

Path to TRL6 [M19-M27]: When feedback from the local CI stakeholders will be gathered about the ENDURANCE strategy draft, we will organise the second European workshop with an **extended Working Group** (**WE2** at M21) and make an evaluation exercise focusing on the cross-border disruption anticipation, management, coordination, and communication. The insights from this workshop (and the results of the initial pilot exercises) will be used for the **improvement of the Strategy**, which will then be evaluated on a local level (**WL3** at M27).

Building upon the discussions, research, developments, and validation in WP1-WP10, we will refine the use cases and associated requirements for reaching TRL6, update the technology designs, and adjust the technical and strategic roadmap relevant for reaching TRL6 (**D4.1** at M21). This will be a baseline for all **improvements in WP5&6 and WP7&8**, which will enable the **second large-scale tests / joint exercises** in WP9&10, bringing the ENDURANCE Services to **TRL6**. Results will be presented in **D10.1&D10.2** at M27.

Path to TRL7 [M28-M36]: Building on the results of the second round of pilots (WP9&10), and on the new inputs of the extended Working Group from the final European workshop (**WE3** at M30), we **will finalise the ENDURANCE Strategy** (**D2.2** at M32). This will help to define reference designs for the ENDURANCE Services and refine our roadmap towards TRL7 (**D4.2.** at M32) and will guide the last phase of the developments and **improvements in WP5&6 and WP7&8**, resulting in the final data space, final versions of other enablers, and in the final implementation of the ENDURANCE Services (**D6.1** and **D8.1&D8.2** at M34). These will be used for the **final large-scale tests / joint exercises** in WP9&10, bringing the ENDURANCE Services to **TRL7**. Results will be presented in **D10.3&D10.4** at M36.

The developments, deployments, and validation activities will be **assessed from the compliance perspective**, and the results will be reported in **D12.3** at M32, which will include **policy recommendations**.

Path to impact [M01-M36]: WP11 will start with the set-up of the **project brand** and **communication channels** by M03 (**D11.1**). By M12, WP11 will release the refined impact generation strategy (**D11.2**). Afterwards, based on this strategy and by following the maturity of the project results, WP11 will focus on promoting project activities and results, disseminating knowledge, contributing to relevant standardisation activities and European policy making, defining result-specific business models and business plans, and developing a sustainability roadmap. Updated strategy and reports from these outcomes will be reported at M21 (**D11.3**) and M36 (**D11.4**).

In **T11.5**, we will define an approach for the evaluation of the ENDURANCE impacts (presented in **D11.2**) and then use this approach to continuously quantify and qualify the impacts made by the project activities and results (presented in **D11.4**). All the impact generation activities will provide guidance to developments in WP1-WP10.

Coordination [M01-M36]: After the project kick-off, we will prepare the **project handbook** (**D12.1** by M03) to formalise the organisational structure of the project, specify management procedures, present internal and external project bodies, and define their responsibilities. The consortium will contribute regularly to **progress reports** (as per the rules set in the Grant Agreement). Under the umbrella of **T12.1**, the consortium will regularly synchronise to **(1)** ensure alignment of the project work with the roadmap set in **T3.5&T4.5**, **(2)** ensure a high quality of project outcomes as defined in **T12.2**, and **(3)** effectively manage risks identified in **T12.2**. Moreover, WP13 oversees management of any relevant security issues and requirements (including security reviews and clearances; **T12.2**). Finally, as already mentioned above, WP12 includes continuous ethical and legal analysis of the project to help guide the partners in their innovation activities. This includes organising a **research ethics and compliance workshop** (during M01-M03) to establish guidelines for research ethics and compliant data management.

3.1.2. Summary of Costs

'Subcontracting costs' items

Participant Number/Short Name		
	Cost (EUR)	Description of tasks and justification
Subcontracting	Not applicable	Not applicable

3.2. Capacity of Participants and Consortium as a Whole

3.2.1. Competencies and Complementarity

The consortium includes **22 beneficiaries and 1 affiliated entity** with **interdisciplinary knowledge** from **7 EU MS** (Belgium, Germany, Greece, Ireland, Italy, Romania, Slovenia), which will facilitate strong international collaboration. Partners bring together important skills on various disciplines that include **SSH** (ethics, law, sociology, economy, business development, communication; see Section 1.2.5) and **open science practices** (see Section 1.2.7).

The topics addressed by ENDURANCE integrate a variety of concepts and thus require a combination of specific skills. The consortium includes partners that have **the exact set of all needed competences** to achieve the defined objectives and impacts. **The entire Innovation Team also has extensive experience with INFRA and CS projects**, not only as participants but as partners **with significant roles** such as the project coordinator, technical coordinator, large-scale pilot lead, impact generation lead, and/or policy making lead.

Further, all consortium partners have a documented track record in different areas relevant for the project as well as **previous collaborations**, which will ensure timeliness and quality of results within the allocated budget, as well as their high exploitation potential and wide impact. Partners' competencies (illustrated below) are deeply integrated within individual WPs, but also span across all WPs, ensuring **strong collaboration and cooperation** and enabling **partner interchangeability** to reduce potential performance risks.

Competence		CI RESILIENCE								DATA SCIENCE (incl. ML & AI)								SW ENGINEERING							TRANSVERSAL ASPECTS									
Team	Partner	Stakeholder Engagement	CI	Cyber-Physical Security	Penetration Testing	Interdependency Modelling	Risk Assessment	Business Continuity	Large-Scale Tests	DataOps	Data Protection	Data Modelling	Data Exchange	Data Analytics	Federated ML	Data Visualisation	Data Governance	SW development	System Integration	Edge Computing	Blockchain / DLT	Immersive Tech	Training Tools	User Experience	Legal Compliance	Ethics	IPR Management	Communication	Dissemination	Standardisation	Policy Making	Business Development	Public	Project Management
INNOVATION TEAM	EVI-RO	x	x	x	x		x				x	x		x				x	x	x			x					x	x	x		x		x
	EVI-DE	x	x	x						x	x	x	x	x		x	x	x	x	x		x	x	x				x	x	x		x		x
	ENG	x	x	x		x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				x	x	x		x		x
	SYN	x	x	x		x	x		x	x	x	x	x	x	x		x	x	x	x	x			x				x	x	x		x		x
	SBT	x	x	x			x			x	x	x	x	x		x	x	x	x				x	x				x	x			x		x
	ICCS	x	x	x						x	x	x	x	x		x	x	x	x	x		x						x	x			x		x
	ICS	x	x	x	x	x	x	x	x		x						x											x	x	x	x	x		x
CI TEAM	AKOS	x	x	x			x	x																	x			x	x		x		x	x
	URSIV	x	x	x			x	x																	x			x	x		x		x	x
	TS	x	x	x	x		x	x																				x	x				x	x
	ELES	x	x	x			x	x																				x	x				x	x
	DNSC	x	x	x			x	x																	x			x	x		x		x	x
	MoH	x	x	x			x	x																	x			x	x		x		x	x
	DGPI	x	x	x			x	x																				x	x				x	x
	CGDM	x	x	x			x	x																				x	x				x	x
	FVG	x	x	x			x	x																	x			x	x		x		x	x
	INS	x	x	x	x		x	x			x			x		x	x		x						x			x	x				x	x
	RDFA	x	x	x			x	x																	x			x	x		x		x	x
	RDFW	x	x	x			x	x																	x			x	x		x		x	x
	EYDAP	x	x	x			x	x																				x	x				x	x
SSH TEAM	TLX	x					x				x						x								x	x	x	x	x		x	x		x
	DBC	x																							x	x	x	x	x	x	x	x	x	x
	CCL	x																										x	x	x	x	x		x

3.2.2. Roles and Resources

The consortium comprises multidisciplinary partners with a variety of skills needed to achieve project objectives. Each partner **has a clear role in the project** to conduct their planned work.

The project will be overseen and guided by the **Project Steering Committee (PSC)** comprising the following roles: Project Coordinator (**EVI-RO**), Technical Coordinator (**ENG**), Data Manager (**SYN**), Cooperation Manager (**ICS**), Ethics and Compliance Manager (**TLX**), and Impact Strategy Manager (**DBC**). The **PSC** will oversee and steer the administrative, financial, technical, and strategic project coordination in line with FAIR data management principles, applicable ethical standards, and relevant regulatory frameworks, while maximising the impact. Their vast expertise and know-how in complex research projects will **(i)** ensure active and continuous **engagement** of all the relevant CI stakeholders, **(ii)** facilitate scientific, technical, and strategic **synergies and alignments** across WPs, **(iii)** ensure effective, legal, and compliant **data management**, **(iv)** ensure timely delivery and high quality of project **outcomes**, and **(v)** facilitate fast and wide **exploitation** of project results.

Partners with expertise in CI resilience (**partners #1-#6**) will form the **Innovation Team**. Their main contributions will be in developing the ENDURANCE strategy, tools, and services. In doing so, they will be supported by the end users (**partners #7-#19**), the group of CI authorities and operators forming the so-called **CI Team**, who will share their experience, best practices, needs, and expectations, and will evaluate and validate the ENDURANCE results. The SSH experts (**partners #20-#22**), forming the **SSH Team**, will help ensure that the project results adhere with the highest ethical standards and regulatory frameworks, address the needs of our society, consider impacts to our economy (to ensure sustainable growth), and are continuously promoted and disseminated to target audiences.

Specific **roles and responsibilities of the ENDURANCE Teams are presented in the table below**.

Note: All Teams will support the **PSC** in co-designing, refining, and implementing the technical and strategic roadmap, as well as in the evaluation and uptake of project results.

The consortium will aim to achieve a **good gender balance** in the R&D teams, will ensure inclusion, and will create equal opportunities for women, men, and gender-diverse individuals, as a universal remedy against taking hard-to-identify sex/gender biased decisions and approaches during implementation of the project.

Role	INNOVATION TEAM (partners #1-#6)	CI TEAM (partners #7-#19)	SSH TEAM (partners #20-#22)
Cross-organisation / -sector / -border **cooperation and collaboration enhancement**.	x	x	x
Methods, models, and technologies for the **analysis of cross-x interdependencies, vulnerabilities, threats, hazards, risks**.	x	x	x
Development of disruption assessment, anticipation, and preparedness strategies, i.e., **business continuity planning**.	x	x	x
Organisation and coordination of **cross-x, large-scale stress tests and exercises**.	x	x	
Methods, models, and technologies for **data preparation** (cleaning, modelling, harmonising, protecting).	x		
Architectures and technologies for **data space** integration and utilisation (data space, connectors, APIs).	x		
Techniques and tools for efficient, scalable, secure **data management** (DataOps).	x		
Methods, models, and technologies for **secure data exchange and federated data processing** (including AI-based).	x		
Frameworks for transparent, holistic, and proactive **data governance**.	x		
Metrics, methodologies, and technologies for dynamic, **cross-x risk & resilience assessment**.	x		
Techniques, scenarios, and technologies for **immersive education and training** on CI resilience.	x		
CI resilience policy design, awareness, and improvement (ethics, law, standards, policy).	x	x	x
Socio-economic assessment of project outcomes and impacts.	x	x	x
Results **demonstration** (including user training), **promotion**, and **uptake** (including IPR management).	x	x	x

In terms of the **key resources**, the **Innovation Team** and the **CI Team** will provide all the necessary technological resources, namely **(i) data** (related to the CIs, essential services, interdependencies, risks), where proprietary data will be provided by the CI Team and open data will be explored and gathered by the Innovation Team, **(ii) computing infrastructure**, where the CI/CD environment for the research, developments, and pre-pilot testing will be provided by **ENG**, cloud resources for local pilot deployments by CI operators, and other equipment and services (servers, sensors, SW licences, etc.) will be purchased and ensured by partners needing them, and **(iii) project management tools** (collaborative platform, communication tools, etc.) will be provided by **EVI-RO**. The **SSH Team** will design, develop, print, and distribute the promotion material (brochures, posters, videos, website, etc., see Section 2.2).

All partners will contribute with their **knowledge, experience, and relevant networks** required to reach excellence of project outcomes and achieve the expected impacts.

3.2.3. Industrial / Commercial Involvement

ENDURANCE has a large industrial commitment with **3 large enterprises** (EVI-RO/-DE, ENG) and **5 European technology and consultancy SMEs** (SYN, SBT, TLX, DBC, CCL) contributing to the R&D efforts and driving the industrial exploitation and commercialisation of results. They will be supported by **7 EU MS authorities** (AKOS, URSIV, DNSC, MoH, FVG, RDFA, RDFW) and **6 CI operators** (TS, ELES, DGPI, CGDM, INS, EYDAP) from the **public and private domain** who will co-design project results, and thus significantly contribute to their maturity, usability, and scalability across different sectors and EU countries.

Large enterprises cover the key parts of the ENDURANCE value chain. They are visible global players with large customer bases, which will ensure **great visibility and successful exploitation of project results**: **EVI-RO/-DE** is the global leader in digital transformation and a key player in the cybersecurity market. EVI-RO will coordinate the project (**WP12**) and will lead the second phase of the ENDURANCE services development (**WP7&WP8**). **ENG** is a leading European IT solutions and services group with strong international presence and expertise, offering innovative and added-value solutions to a wide range of public and private organisations. ENG, being the Technical Coordinator, will drive the technical and strategic roadmap (**WP3&WP4**).

SMEs will drive the technical developments in the project, thereby ensuring that all **R&D activities are focused on the market needs and that the results mature quickly, are flexible and competitive**: **SYN** is a technology provider that innovates, implements, and explores industry's most advanced technologies (including in data science, machine learning, and cryptography), and translates them into value for customers. SYN will act as the Data Manager (**T5.1&T6.1**) and will lead the second phase of the ENDURANCE enablers development (**WP5&WP6**). **SBT** is a leading brand in the field of comprehensive risk management in Slovenia. SBT will bring to the project their **risk management platform**, one of the key project technologies, and will lead the first phase of the ENDURANCE services development (**WP7&WP8**). **TLX** is a leading niche law firm specialised in the legal aspects of information technology, privacy and data protection (GDPR), intellectual property, and media and electronic communications. Striving to match law and innovation, **TLX** will, as Ethics and Compliance Manager, support the analysis of and adherence with relevant laws (**T12.3**). **DBC** is a business consulting firm offering advisory services to global private and public organizations in all sectors. DBC will, as the Impact Strategy Manager, coordinate the project efforts in exploiting and managing IPR of project results (**T11.1**,**T11.4**). Finally, **CCL**, as one of Ireland's longest-running communications companies, has become a household brand name for media, public relations, communications, and business / management training, and development. CCL will coordinate the communication and dissemination efforts (**T11.2**, **T11.3**).

CI authorities and operators will be the co-creators, first adopters, and promoters of ENDURANCE. From their hands-on experience, they will provide the consortium invaluable insights, making it easier for the developed technology to be put to practice in **real-world scenarios and scale across Europe**.

3.2.4. Affiliated Entities

Eviden Germany GmbH, part of the Eviden Group and a subsidiary of the Atos Group, stands out as a European leader in data-driven, trustworthy, and sustainable digital transformation. With an Eviden group annual revenue of approximately EUR 5 billion, the company specializes in digital transformation and offers a comprehensive range of solutions across various sectors, including cybersecurity, cloud computing, and advanced computing. This strategic positioning highlights its commitment to advancing digital infrastructure and services across Europe.

Eviden Germany GMBH is part of the same group as the project coordinator Eviden Technologies SRL.

The role of Eviden Germany GmbH in the project will be related to leading the activity of Digital Twins for Interconnected Essential Services.

The total cost for the affiliated entity is 146,875 EUR, corresponding to a grant amount of 102,812.50 EUR.

3.2.5. Role and budget of Associated Partners

Not applicable.

4. Ethics self-assessment

4.1. Ethical dimension of the objectives, methodology and likely impact

The ENDURANCE proposal comprises certain ethical challenges, which are in part due to the general concept of applying systematic and automated risk monitoring measures to activities that can impact EU citizens, and in part due to the planned pilot scenarios.

The general concept behind ENDURANCE is to extend the cooperation and collaboration mechanisms between CI stakeholders, thus enhancing the maturity of cybersecurity and cyber resilience strategies, and strengthening the protection of interconnected essential services. With respect to ethical impacts, the pilots were selected for their societal relevance and impact, since successful piloting can contribute to the availability and quality of critical infrastructure and the services that rely on them, including with respect to environment, disaster management and personal health. The ethical benefits are thus clear.

However, as a part of the methodology for achieving this anticipated impact, ENDURANCE also aims to develop datasets, registries, methodologies, technologies, and services for secure sharing and federated

processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness. The focus of ENDURANCE is not on increasing the monitoring of EU citizens, but rather to ensure that data monitoring practices are improved, streamlined, and effectively secured. None the less, information collecting sharing is expected to be enhanced, which implies that the ethical risks inherent to this objective must be monitored and managed.

Specifically, these risks include (1) an unintended increase of the levels of monitoring and evaluation of EU citizens, which can impact their privacy in a manner that was not intended; (2) needlessly extensive data sharing of personal data with stakeholders that do not strictly require it; (3) ineffective use of pseudonymization and anonymization techniques in manner that needlessly exposes personal data; (4) insufficient control over personal data usage by recipients, resulting in usage that is no longer strictly limited to the ENDURANCE proposal's remit; and (5) unintended profiling and decision-making that negatively impacts EU citizens, as a result of the misapplication of AI technologies.

It should be noted that none of the risks above are expected to materialize in practice, since the ENDURANCE project is emphatically *not* intended to focus on personal data. Wherever possible – and this will be nearly universally the case in the context of the ENDURANCE project – collected and exchanged data will focus on data pertaining to technical systems, networks and infrastructure, at the exclusion of any data that could be linked to individual persons (i.e. the targeted data sets focus on non-personal data, where data protection and privacy issues cannot reasonably occur). The project partners have no interest in obtaining access to each other's personal data, nor to engage in data collection that is outside of their legal remit.

None the less, the partners will identify and manage these risks in the course of the project. This is particularly important in the meso and micro pilots. As was explained in the proposal, the targeted scope of the pilots includes Public Administration and (Drinking & Waste) Water Management, as well as Digital, Energy, and Health. The focus of the pilots is never on individual (personal) citizen data, but rather on infrastructural data and on CER/risk related data. ENDURANCE does not require or envisage that personal data in the pilots is exchanged between partners.

However, the pilots do require an examination of available data at the pilot sites, and the source datasets could contain personal data. While that personal data is not the focus of ENDURANCE, this does create a data protection risk to be managed: personal data (e.g., related to a household's energy consumption, a patient's health records, or their waste production) may not be processed contrary to the GDPR.

ENDURANCE will favour piloting on the basis of non-personal data exclusively wherever possible; and where the objectives of a pilot inherently require a processing of personal data, priority will be given to using fake or synthetic data where possible, so that no impacts on actual persons can be expected. Only as a matter of last resort will actual personal data used, and in those instances, the safeguards referenced below will be applied to ensure compliance with the GDPR and other legal frameworks.

Multiple methodological safeguards will be implemented in the ENDURANCE action, both at the level of the framework as a whole, and at the level of individual scenarios. Two specific tasks are defined to identify and manage risks:

- T12.2 Quality Assurance & Risk Management. This includes the preparation of templates, guidelines, protocols, and tools for quality assurance, risk management, and security management, and the continuous management of quality assurance, risks, and security.
- T12.3 Ethics & Legal Aspects. This includes an analysis of relevant legal and ethics aspects, drafting of legal and ethical compliance guidelines, and consulting, assessing, and monitoring alignment with legal and ethics requirements.

These tasks will run throughout the project, and will ensure a consistent and homogenous approach to ethics and fundamental rights. Within ENDURANCE, data protection by design and by default will be applied as guiding principles in all pilots. Each pilot will undergo a data protection impact assessment and a human rights assessment, to determine fundamental risks rights, and to ensure that appropriate

mitigation measures are taken. All piloting activities will be supervised by a designated, identified and duly qualified data protection officer (DPO) that satisfies the legal requirements of the GDPR. In this way, accountability is built into ENDURANCE.

4.2. Compliance with ethical principles and relevant legislations

ENDURANCE is fully aware of the underlying ethical, privacy, safety and trust issues that arise in CI protection, and addresses these both organizationally, and via dedicated tasks.

Organizationally, ENDURANCE has foreseen continuous ethics and privacy monitoring measures, via the creation of a specific ethics and legal compliance task (12.3). This task is charged with establishing ethics guidelines and procedures, including prior approval requirements before piloting can initiate. An Advisory Board will be created under T12.1, so that the project's execution will also be guided by external recommendations.

By establishing clear procedures early on and integrating external evaluation, ENDURANCE aims to give ethics compliance a central place in the project and expects to tackle any potential ethics issues. This will include traditional measures, such as creating informed consent forms, procedures for collecting consents, procedures for selecting participants in the scenarios, and so forth.

Beyond these organizational approaches, more targeted measures will also be required, such as the completion of a data protection impact assessment (DPIA) that satisfies the requirements of the GDPR; and this will be enriched with a broader human rights impact assessment (HRIA) that will factor in impacts on other fundamental rights than privacy and data protection – such as e.g., human dignity and autonomy. At the use case level, specific safeguards will also be examined to ensure that the project is acting in a way that is both ethically sound and legally compliant. This also entails the identification of legal compliance requirements beyond those of the GDPR, including e.g., for emerging rules under the proposal for an AI regulation (the proposed EU AI Act) and the proposed Regulation on the European Health Data Space, the Data Governance Act, and other proposed legislation such as the Data Act, that may impose specific requirements on data collection and data sharing.

A specific dedicated legal partner will continuously monitor legislative changes at the EU level as a part of Task 12.3, and propose harmonized approaches across piloting scenarios, as well as scenario-specific recommendations to address scenario-specific concerns.

Finally, formal data protection compliance assurances also need to be established, including privacy policies, data processing agreements, and anonymization/pseudonymization policies, taking into account available guidance from data protection authorities. The issue of transfers of personal data outside of the EU also should be evaluated at the use case level. In principle, this task should not be excessively daunting, as it is likely that the project can be executed without exporting pilot level personal data outside of the EU. In the eventuality that this proves infeasible, use will be made of Commission-approved Standard Contractual Clauses, tailored to the project. Data transfers will be monitored to ensure compliance.

At the use case level, we will also evaluate whether there are any applicable additional ethical or legal requirements in specific countries, including e.g., data localization requirements or prior approvals/authorisations from ethical committees or specialized authorities; and where needed bespoke legal agreements will be established to cover pilot specific issues such as car safety, medical device regulations, and copyrights.

Beyond the legal aspects, the operational provision of safety, security and trustworthiness is explicitly foreseen in the ENDURANCE workplan (T12.1 – Quality Assurance & Risk Management), so that ethical assurances are not only dealt with at the legal and policy level. Indeed, a core objective of ENDURANCE is ensuring that ethics is embedded into the technology itself.

5. Summary of the Project Security Issues

The project concerns critical infrastructure, invoking real-life scenarios for the continuity of the interconnected essential services, including analysis of threat assessments, thereby raising security concerns.

5.1. Sensitive Information with Security Recommendation

Public versions of the deliverables, D8.2 ENDURANCE Services (formerly D4.2), D9.3 First Pilot Report (formerly D5.2), D10.2 Second Pilot Report (formerly D5.3), D10.4 Final Pilot Report (formerly D5.4) should be approved by the SAB prior to dissemination.

Sensitive information with security recommendation			
Number and name of the deliverable	**Name of the lead participant**	**Date of production**	**Name of entity authorised for access**
D3.2 Roadmap Towards TRL5 (formerly D2.2), D4.1 Roadmap Towards TRL6 (formerly D2.3), D4.2 Roadmap Towards TRL7 (formerly D2.4): These reports will present the requirements, designs, strategic and technical roadmap towards TRL5 / TRL6 / TRL7. The last iteration (D4.2) will include reference designs of the ENDURANCE solutions.	ENG	M12 / M21 / M32	All partners (on a need-to-know basis), EC
D5.1 Enablers Prototypes (formerly D3.1): This report will present the initial prototypes of the ENDURANCE enablers.	ICCS	M15	All partners (on a need-to-know basis), EC
D6.1 ENDURANCE Enablers(formerly D3.2): This report will present the final prototypes of the ENDURANCE enablers (data space, SW components and modules, interfaces).	SYN	M34	All partners (on a need-to-know basis), EC
D7.1 Service Prototypes (formerly D4.1): This report will present the initial prototypes of the ENDURANCE services.	EVI-DE	M15	All partners (on a need-to-know basis), EC
D8.2 ENDURANCE Services (Sensitive, formerly D4.2): This report will present the final prototypes of the ENDURANCE services (for data sharing, risk management, and training and simulations) and advanced dashboards.	EVI-RO	M34	All partners (on a need-to-know basis), EC
D9.1 Test Designs and Plans (formerly D5.1): This report will present the designs of / plans for stress tests and large-scale exercises.	INS	M12	All partners (on a need-to-know basis), EC
D9.3 First Pilot Report (Sensitive, formerly D5.2), D10.2 Second Pilot Report (Sensitive, formerly D5.3), D10.4 Final Pilot Report (Sensitive, formerly D5.4) : These reports will provide high-level summaries from the three pilot execution cycles for all pilots.	INS	M18 / M27 / M36	All partners (on a need-to-know basis), EC