



OCTOBER 2026 INTAKE

The MBA for professionals who will lead secure digital transformation in Europe, not just respond to cyber risk.

18 months. 3 semesters.

The strategy, governance, AI, regulation, risk, and management capabilities to build cyber-resilient organisations, starting in October 2026.

DURATION

18 months

Structured across 3 semesters

CREDITS

90 ECTS

LANGUAGE

English

DELIVERY

Online with hybrid elements

AWARD

MBA Degree

EQF/ISCED Level 7 /
AMBA Accredited

Contents

Faculty and teaching ecosystem	03
Programme positioning	04
Target audience and candidate fit	05
Welcome messages	06
About École des Ponts Business School	07
Heritage and quality	08
Research in action	09
MBA in Advanced Cybersecurity Technologies & Governance	10
Why now	11
Learning outcomes	12
18-month journey	13
Semester 1 pathway	14
Semester 2 pathway	15
Semester 3 pathway	16
Curriculum architecture	17
Learning experience	18
Virtual Campus	19
European research connection	20
Career directions	21
Admissions process	22
Fees and eligibility	23
Application preparation	24

KEY FACTS

Programme snapshot

START
Early October
2026

DURATION
18 months

CREDITS
90 ECTS

LANGUAGE
English

DELIVERY
Online with hybrid
elements

AWARD
MBA Degree

Full tuition-fee waiver for eligible applicants.

Eligible applicants who are citizens of EU Member States or Digital Europe Programme countries will receive a full waiver of tuition fees, subject to admission and confirmation of eligibility. The waiver applies to tuition fees only. A non-refundable application fee is payable by all applicants. Admitted applicants must also pay the applicable admission/registration fee.

Applicants who do not meet the tuition-fee waiver criteria are responsible for all applicable fees, including tuition fees.

The MBA in Advanced Cybersecurity Technologies & Governance at École des Ponts Business School is accredited by the Association of MBAs (AMBA). Accreditation denotes the highest standard of achievement in postgraduate business education and is globally recognised by employers and students.



FACULTY AND TEACHING ECOSYSTEM

A European teaching ecosystem behind your MBA journey

Our MBA is delivered through a European cybersecurity education ecosystem combining academic leadership, applied research, technical expertise and industry insight. Through this network, participants engage with the strategic, regulatory and organisational dimensions of cybersecurity, including AI-enabled threats, digital trust, privacy, cyber governance, resilience and secure digital transformation.



6

academic university
partners



**Research and
industry**

contributors



**Multidisciplinary
European
faculty**





A DISTINCTIVE MBA

A specialised MBA in cybersecurity governance and digital resilience

This is not a traditional MBA with a cybersecurity module added on. It is an applied MBA built around the technologies, risks, regulations, governance models and leadership capabilities defining the next phase of digital competitiveness.

This programme was designed for two groups of professionals: cybersecurity and IT professionals who are ready to move from technical execution into executive leadership, and leaders in risk, governance, compliance, privacy, insurance, policy and digital transformation who need to understand cyber risk deeply enough to govern it credibly. For both groups, this is where cybersecurity becomes a board-level management capability.

Strategic leadership

Executive cyber leadership

Lead cybersecurity strategy, governance, and digital trust at organisational and board level.

Emerging technologies

AI and emerging threat awareness

Understand how AI, automation, and new attack surfaces are reshaping cyber risk.

Cyber governance

Governance, risk and compliance

Connect cybersecurity with regulation, privacy, insurance, policy, and organisational accountability.

Organisational resilience

Resilience-focused decision-making

Build the capability to prepare, respond, recover, and lead through cyber disruption.

IS THIS MBA FOR YOU?

Designed for professionals building cyber-resilient organisations

This MBA is built for experienced professionals who need to connect cybersecurity, business strategy, risk management, governance, compliance and business continuity in the digital age.

Cybersecurity and IT professionals

Move from technical or operational roles into strategic cyber leadership, governance and executive decision-making.

Risk, compliance and governance managers

Strengthen capability in cyber risk, regulatory readiness, internal controls, assurance and board-level reporting.

Business continuity and resilience professionals

Prepare organisations to anticipate disruption, respond to incidents, protect operations and recover with confidence.

Technology and digital transformation leaders

Lead secure digital transformation, AI adoption, technology strategy and cyber-resilient innovation projects.

Insurance and financial services professionals

Understand cyber risk, cyber insurance, digital trust, fraud prevention, financial resilience and business continuity.

Consultants, advisers and venture builders

Support organisations or build solutions in cybersecurity, governance, AI, digital trust, privacy and secure technology.

Good fit: ideal for professionals who want to lead cyber resilience and digital trust, not simply study cybersecurity tools.



WELCOME MESSAGES

Leadership perspectives



Business education has largely failed to keep pace with the cybersecurity challenge. Technical cybersecurity courses exist. Compliance programmes exist. General management MBAs exist. But a rigorous programme connecting cyber risk, AI, regulation, governance, digital trust, and executive leadership has been missing. This MBA fills that gap. Built on the engineering heritage of École des Ponts and designed for professionals operating at the intersection of technology, strategy, risk, and organisational transformation, it treats cybersecurity for what it is: a core business leadership capability in the digital age.

Alon Rozen
Dean, École des Ponts Business School



Cybersecurity is one of the defining management challenges of our time. It requires leaders who can bridge strategy, technology, regulation, risk, finance, insurance, privacy, and organisational change while turning research-informed insight into action. Developed within the EU-INSPIRE project, this MBA reflects EPBS's commitment to applied postgraduate management education for professionals operating in technology-intensive and regulated environments. Throughout the 18-month programme, participants explore cyber risk, digital trust, AI-enabled threats, privacy, governance, cyber insurance, operational resilience, industrial cybersecurity, incident response, and international cyber policy. The program aims to equip them with the judgement and capabilities needed to lead credible cybersecurity governance and digital resilience across organisations and ecosystems.

Giorgos Demetriou
Associate Dean of Research and Programme Director, École des Ponts Business School



Cybersecurity has evolved from a technical concern into a strategic leadership challenge. Organisations today must navigate a complex landscape shaped by digital transformation, AI, regulation, and increasing cyber threats. Success depends on leaders who can connect technology, governance, risk management, and business strategy. Developed within the EU-INSPIRE project, this MBA was designed to develop exactly these capabilities. By combining academic excellence, applied research, and practical industry perspectives, it prepares professionals to make informed decisions, build organisational resilience, and foster digital trust in an increasingly interconnected world. I am pleased to contribute to a programme that equips the next generation of leaders to address some of the most important challenges of the digital age.

Costas Lambrinoudakis
Director, Systems Security Laboratory, University of Piraeus

ABOUT THE SCHOOL

École des Ponts Business School: management education for complex business transformation

École des Ponts Business School has a pioneering heritage in international business education, leadership, and impact. Founded in 1987 and connected to the historic École Nationale des Ponts et Chaussées, the school carries forward a bridge-building tradition: connecting industrial disciplines, cultures, technologies, and people to help leaders build a better future.

FOUNDED
1987

LOCATION
Paris, France

ACADEMIC ORIENTATION
**Postgraduate
management**

DISTINCTIVE LENS
**Engineering, policy,
research-driven innovation
and business administration**



HERITAGE AND QUALITY

Rigorous by heritage. Relevant by design.

277 years of academic excellence

École des Ponts Business School is built on the foundation of École Nationale des Ponts et Chaussées, founded in 1747, one of the world's oldest and most respected institutions of higher education. That heritage of precision, systems thinking, and rigorous inquiry runs through everything we do.

Applied to real decisions, not hypothetical frameworks

Every course, every assessment, and every project is designed around real organisational challenges. You graduate with capabilities you have already used, not frameworks you have only studied.

Built for professionals leading transformation

Post-experience learning for senior professionals who need integrated business, technology, and leadership capability to drive complex change and who cannot afford to stop working while they build it.



AMBA Accredited

Recognising high standards in postgraduate business education and international management learning.



Qualiopi Certified

Reflecting quality of professional training processes, learner support and educational delivery.

RESEARCH IN ACTION

Learn from research that is happening right now.

This MBA is not built on archived case studies. It is developed in the context of the EU-funded EU-iNSPIRE project, connecting you to a live European network of academic partners, cybersecurity practitioners, industry organisations, and innovation projects working on the same challenges you will face as a leader: cyber risk, AI-enabled threats, governance, privacy, regulation, digital trust, and organisational resilience.

Current cyber research, not yesterday's frameworks

The curriculum is informed by EU-iNSPIRE and related Digital Europe activity, ensuring that what you study reflects current developments in AI-enabled threats, digital trust, privacy, cyber governance, and operational resilience.

Access to a European cybersecurity education network

As a participant, you connect to academic partners, technical experts, industry contributors, and practitioners across Europe, a professional network built around the resilience challenges you are training to lead.

From insight to application

Research and technical insight are translated directly into learning tools, cyber scenarios, governance frameworks, and applied project challenges, so you use current knowledge to make real organisational decisions.

Research centres and labs.

Circular Economy Research Center, the INSPIRE Competence Lab and the Smart Health & Social Innovation Lab as examples of EPBS research activity.

European project portfolio.

Projects such as 3D-CIRCULAR and EU-INSPIRE connect curriculum design, applied research, digital skills and professional upskilling.

Discover

Identify emerging cybersecurity, AI, governance and resilience challenges through research, projects and partner collaboration.

Translate

Turn research and technical insight into management frameworks, learning strategies and organisational solutions.

Apply

Help learners use research-backed knowledge in professional contexts, from cyber governance roadmaps to resilience strategies and applied business projects.



Why professionals choose this MBA

Most professionals working in cybersecurity, risk, compliance, privacy, AI, or digital transformation face the same challenge: cyber decisions are no longer only technical, but many organisations still manage them in silos. This MBA closes that gap by integrating cybersecurity, AI, governance, regulation, risk and business strategy into one applied learning journey.

1

Cyber risk as a business priority

Translate cyber risk into executive-level decisions that protect trust, continuity and value.

2

Designed for experienced professionals

Study while working, with flexible online learning and applied executive-level content.

3

Governance, AI and regulation together

Connect cybersecurity, AI, privacy, compliance, digital trust and organisational resilience.

4

Applied to real organisational challenges

Use cases, cyber scenarios, labs and projects to turn learning into leadership capability.

5

Connected to a European innovation ecosystem

Developed in the context of EU-INSPiRE project, supporting Europe's cybersecurity skills and digital resilience agenda.

October 2026 cohort forming now |
Tuition-free for EU/DEP eligible applicants

WHY THIS MBA, WHY NOW

Build cyber-resilient organisations in the digital age

Organisations are under pressure to become more secure, resilient, transparent and accountable. The leaders who can connect cybersecurity, governance, AI, regulation, risk, insurance and operational change will be central to the next phase of digital competitiveness.

Core message: cybersecurity is now a management capability, not only a technical function.

1

Cyber risk is board-level risk

Cyber incidents affect reputation, operations, legal exposure, business continuity and stakeholder trust.

2

AI is changing the threat landscape

AI-enabled threats, automation, adversarial machine learning, deepfakes and model governance are reshaping cyber risk and digital trust.

3

Regulation is intensifying

GDPR, NIS2, cyber resilience expectations, sectoral obligations and emerging AI rules require leaders who can connect legal, technical and business decisions.

4

Digital trust is a competitive asset

Customers, regulators, investors and partners expect organisations to demonstrate resilience, accountability and credible assurance.



WHAT YOU WILL LEARN

Turn cybersecurity, governance and digital trust into organisational resilience

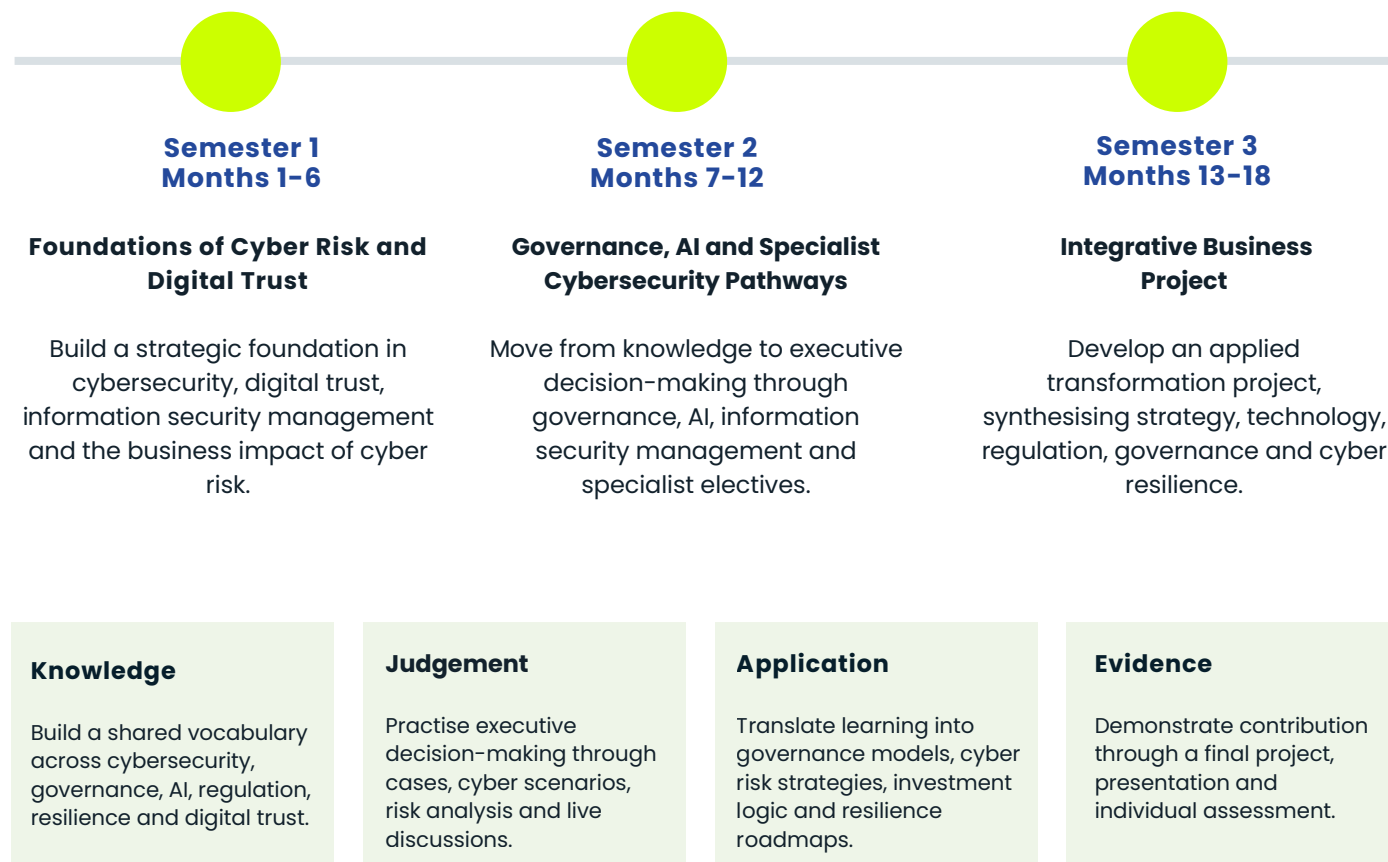
- Evaluate cybersecurity as a strategic business and societal risk.
- Turn technical, legal and threat information into executive decisions.
- Design cyber governance, digital trust and resilience strategies.
- Apply privacy, network, IoT, forensics and industrial cyber knowledge.
- Use risk assessment, threat intelligence and incident response tools.
- Lead responsible innovation at the AI-cybersecurity interface.
- Communicate cyber risk clearly to boards, regulators and teams.
- Complete an applied project on cybersecurity governance or digital resilience.



AN 18-MONTH APPLIED MBA JOURNEY

From cyber risk awareness to applied resilience leadership

The MBA is organised as a cohort-based journey combining cyber leadership foundations, governance and risk strategy, specialist electives, online assessments and an Integrative Business Project.



Semester 1

Foundations

Orientation

Join the MBA Community

- Programme onboarding and academic expectations
- Virtual campus, cohort access and collaboration tools
- Syndicate group formation and peer-learning routines

MILESTONE

Define your professional learning goals and identify an organisational, sectoral or ecosystem challenge relevant to cybersecurity, AI, digital trust or resilience.

Core foundations

Build shared expertise

- Strategic Leadership in Cyber Risk and Digital Trust
- Leading Sustainable Innovation in the AI-Cybersecurity Value Chain
- Select two electives from the available portfolio

MILESTONE

Analyse a cyber risk, governance, technology, privacy or resilience challenge through strategic, regulatory, technical and organisational lenses.

Applied work

Connect theory to practice

- Scheduled synchronous teaching and structured asynchronous learning
- Case analysis, discussion prompts and applied assignments
- Early project framing for later capstone work

MILESTONE

Leave Semester 1 able to explain cybersecurity and digital trust challenges in strategic, regulatory, technical and organisational terms.

Semester 2

Leadership

MBA core

Move into strategic management

- Data Literacy and Information Security Management
- Cybersecurity risk management strategy
- Threat modelling and risk treatment
- Information security policies and culture
- Professional frameworks and career development

MILESTONE

Develop a management case for cybersecurity transformation, including risk logic, stakeholder impact, governance, controls and organisational feasibility.

Elective focus

Tailor your learning

- Select three electives from the available portfolio
- Build sectoral or functional depth aligned with professional background
- Connect elective learning to organisational, market, venture or career objectives

MILESTONE

Confirm a specialist direction that strengthens your contribution to cybersecurity governance, resilience, operations, policy or innovation.

Leadership practice

Apply executive judgement

- Practitioner-informed and faculty-led learning activities
- Syndicate group and project-team work
- Scenario analysis, Incident response and resilience cases
- Cyber governance and strategic decision-making

MILESTONE

Translate cyber risk and digital transformation intent into governance, innovation, assurance, resilience and implementation decisions.

Integration

Project design

Define the challenge

- Diagnose an organisational, sectoral, policy or ecosystem need
- Frame the research question, scope and evidence base
- Agree methodology, stakeholders and intended contribution

MILESTONE

Submit a project proposal and evidence plan for academic supervision.

Executive application

Research, analyse, test

- Apply business research and consultancy methods
- Integrate cybersecurity, strategy, finance, governance, technology, regulation and stakeholder perspectives
- Develop actionable conclusions and recommendations

MILESTONE

Produce draft findings and recommendations supported by evidence, analysis and reflection.

Finalisation

Evidence your contribution

- Complete the Integrative Business Project
- Present to a client-facing or academic panel
- Submit individual reflection, contribution log and viva / supervisor assessment

MILESTONE

Demonstrate integrated MBA-level learning through a research-informed, practice-oriented cybersecurity governance or digital resilience project.

CURRICULUM ARCHITECTURE

Core expertise and specialist pathways

The curriculum combines foundations in cybersecurity leadership, digital trust and information security management with core MBA learning, specialist electives and a major applied capstone project.

Mandatory foundations

- Strategic Leadership in Cyber Risk and Digital Trust
- Leading Sustainable Innovation in the AI-Cybersecurity Value Chain
- Data Literacy and Information Security Management

Integrative Business Project

A 30 ECTS capstone project delivered through an in-company consultancy project, own-company project, or approved applied case/sectoral challenge. Students develop a strategic, governance, resilience or transformation roadmap connected to a real or realistic cyber challenge.

Elective specialisation

- Privacy and Data Protection
- Cybersecurity Governance
- Network Security Management
- IoT Security Management
- User experience in Cyberspace
- Offensive Security Management
- Forensics
- Secure Autonomous Systems
- Cybersecurity: Attack, Defence, and Operational Practice
- Cybersecurity in Industrial Scenarios
- Cybersecurity in the Political Domain: Internal and External Dimensions

By the end of the MBA, participants should be able to: integrate cybersecurity, AI, digital trust, EU/global regulation, governance, business strategy, leadership, risk management and stakeholder communication into viable organisational strategies.

YOUR LEARNING EXPERIENCE

Rigorous, flexible and applied

The programme is structured for working professionals. Asynchronous learning provides flexibility, live sessions create connection, and applied activities turn cyber concepts into management decisions.

01

Live sessions

Engage in synchronous sessions with faculty, practitioners and peers for discussion, application and executive-level analysis.

02

Digital asynchronous learning

Access guided content, readings, exercises, cases, simulations and learning materials through the digital campus.

03

Peer collaboration

Work with professionals from different sectors, functions and countries on shared challenges.

04

Discussion forums

Exchange perspectives, debate real-world challenges and learn through peer discussion and applied insights.

05

Professional relevance

Use assignments, labs and projects to connect learning to your organisation, sector, policy environment or venture.

06

Digital campus support

Access learning resources, collaboration tools, feedback workflows and student support online.

The standard: structured, synchronous, asynchronous and applied learning designed to maintain cohort identity while accommodating working professionals.

VIRTUAL CAMPUS

Where learning becomes a connected journey

Ponts Academy's digital campus is designed to support each stage of the learner journey, from admission and enrolment to coursework, study groups, brain trusts, credentials and alumni connection.

1

Apply

Submit application information and accept your offer.

2

Enrol

Onboard to virtual campus and access your enrolled courses.

3

Learn

Use your digital course player, access live sessions and asynchronous activities.

4

Collaborate

Work with peers, access to various discussion forums and exchange knowledge.

5

Progress

Assess your knowledge, monitor your grades and build a record of learning.

6

Connect

Join the alumni community and grow your professional network.



RESEARCH AND EUROPEAN ECOSYSTEM

A European digital campus for cybersecurity leadership and resilience

The MBA is developed in the context of Project 101190054 – EU-iNSPIRE, funded by the European Union under the Digital Europe Programme. EU-iNSPIRE focuses on innovative, multidisciplinary, industry-focused cybersecurity education for upskilling and reskilling the EU workforce.

Important distinction

EU project support does not automatically guarantee individual tuition eligibility. Applicants must confirm admissions, funding and fee eligibility through the official process.



EU-iNSPIRE



**Co-funded by
the European Union**

CAREER DIRECTIONS

Prepare for leadership roles in cyber-resilient organisations

This MBA prepares professionals to bridge business strategy and cybersecurity, helping organisations protect digital assets, manage information security risks, maintain business continuity and build digital trust.

C-level cybersecurity leadership

- Chief Information Security Officer / CISO-track roles
- Cybersecurity Director
- VP Cybersecurity and Digital Trust

Cyber risk and governance

- Cyber Risk Manager
- Cyber Governance Manager
- GRC Manager

Business continuity and resilience

- Business Continuity Manager
- Digital Resilience Lead
- Incident Response Manager

Secure digital transformation

- IT Project Manager
- Secure Digital Transformation Lead
- Technology Risk Manager

Compliance and data protection

- Compliance Officer
- Privacy and Data Protection Manager
- Information Security Assurance Lead

Consulting and advisory

- Cybersecurity Consultant
- Security Strategy Adviser
- Digital Risk Consultant

ADMISSIONS

A selective process for experienced professionals

The admissions process is designed to evaluate academic readiness, professional experience, motivation and programme fit.

Are you eligible to join the programme?

Academic background

Bachelor's degree or higher from an accredited institution. Any discipline accepted. Technical background not required.

Professional experience

Minimum 3 years of relevant full-time professional experience after graduation by the time the programme starts.

English proficiency

Applicants must demonstrate sufficient English proficiency for master's-level study. IELTS, TOEFL or equivalent evidence may be required where English is not the first language.

Professional reference

At least one professional reference is required, able to assess performance, leadership potential and MBA suitability.

1

**Check
eligibility**

2

**Prepare
documents**

3

**Apply
online**

4

**Complete
interview**

5

**Receive
decision**

6

**Accept
offer**

7

**Begin
onboarding**

École des Ponts Business School is committed to equality of opportunity and diversity. All applications are evaluated fairly and without discrimination on the basis of gender, nationality, ethnicity, disability, or socio-economic background.



FEES AND ELIGIBILITY

Understand tuition-fee waiver eligibility and fee obligations.

Eligible applicants from EU countries and countries participating in the Digital Europe Programme will receive a full waiver of tuition fees, subject to admission and confirmation of eligibility. The waiver applies to tuition fees only. A non-refundable application fee is payable by all applicants. Admitted applicants must also pay the applicable admission/ registration fee. Applicants who do not meet the tuition-fee waiver criteria are responsible for all applicable fees, including tuition fees.

EU and DEP eligible applicants

Tuition-free access for applicants who are citizens of EU Member States and Digital Europe Programme (DEP) countries, subject to admission and eligibility confirmation. The tuition-fee waiver applies exclusively to tuition fees and does not cover the application fee or admission fee.

€100

Application fee

All applicants are required to pay a non-refundable application fee at the time of application submission.

€2,400

Admission fee

Admitted applicants must pay an admission fee to confirm acceptance of the offer and secure their place in the programme.

€45,000

Tuition fee

For applicants who are not citizens of EU Member States or Digital Europe Programme (DEP) countries.

APPLICATION PREPARATION

What to prepare before you apply

Documents

- ✓ Updated CV
- ✓ Diploma and academic transcript
- ✓ Passport or national ID card
- ✓ Professional reference details
- ✓ English language evidence, where required

Before submitting: check the official application deadline, application link and any applicable fees.

How applications are assessed

Academic readiness

Evidence of capacity to succeed in master's-level study.

Professional progression

Experience showing responsibility, decision-making, leadership exposure or organisational accountability.

Motivation and fit

Clear reasons for choosing this MBA and a credible link to future professional goals.





PONTS ACADEMY

An MBA for professionals building secure, resilient and trusted digital organisations.

For programme enquiries, eligibility guidance and application next steps, use the official Ponts Academy website and admissions portal.

VISIT WEBSITE

This brochure is intended for informational and lead-generation purposes only. Programme details, including dates, delivery format, tuition and fees, eligibility criteria, admissions procedures, and application requirements, are subject to change and should always be verified through the official Ponts Academy / École des Ponts Business School sources before application, admission, or enrolment decisions.

The MBA in Advanced Cybersecurity Technologies & Governance at École des Ponts Business School is accredited by the Association of MBAs (AMBA). Accreditation denotes the highest standard of achievement in postgraduate business education and is globally recognised by employers and students.

The EU-INSPiRE project is co-funded by the European Union under the Digital Europe Programme under Grant Agreement No. 101190054. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

