13 January 2026
ESMA65-955014868-12887

ESMA Digital Strategy 2026-2028

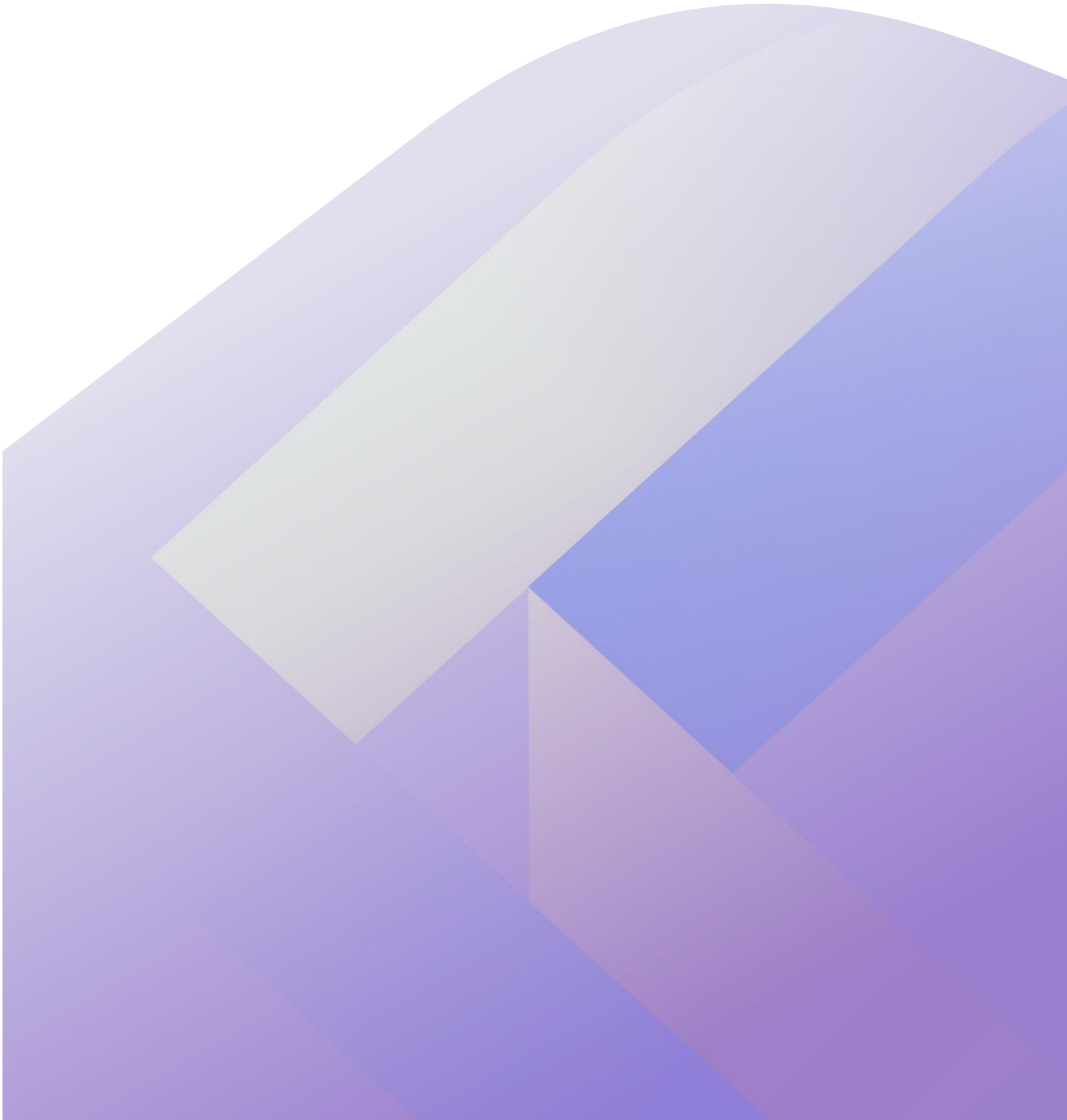


Table of Contents

1 Executive Summary

The ESMA Digital Strategy 2026-2028 supports the broader objectives of ESMA Strategy 2023-2028 and complements the ESMA Data Strategy 2023-2028 by providing a **forward-looking and actionable framework to drive ESMA's digital transformation**. The strategy responds to an evolving landscape marked by expanding regulatory mandates, shifting political priorities, rapid technological advancements, and increasing interdependence with other EU bodies. It aims to **position ESMA as a digitally mature, resilient, and agile Authority**, fully equipped to fulfil its mission of protecting investors, ensuring orderly markets, and safeguarding financial stability within this dynamic and increasingly digitalised environment.

The strategy articulates a clear vision to "***Strengthen the European System of Financial Supervision through secure, innovative, and data-driven digital transformation***". This vision translates into **four Strategic Objectives** that will guide ESMA's digital transformation over the coming years.

Its first objective, "**Build EU Digital Synergies**", aims to promote greater digital integration across ESMA, NCAs, and EU Institutions through shared infrastructure, tools, contracts, and services. This objective supports operational efficiency, improves cross-agency collaboration, and helps reduce fragmentation within the European supervisory digital ecosystem.

Its second objective, "**Enhance Digital Capabilities of the ESFS**", seeks to ensure that ESMA's digital solutions are business-driven, user-centred, closely aligned with regulatory and supervisory priorities, and can be harnessed effectively by well-equipped staff across ESMA, NCAs, and EU Institutions. It includes streamlining processes, enhancing platform usability, enabling better decision-making, fostering innovation through controlled experimentation, and rolling out targeted training programmes.

Its third objective "**Bolster Operational Efficiency**" intends to strengthen ESMA's ICT agility, service delivery, and governance by applying industry best practices, improving vendor and financial management, and standardising and automating processes. The goal is to ensure ICT resources are scalable, resilient, and strategically aligned.

Its fourth and last objective, "**Establish a Best-of-Breed Secure Ecosystem**", is designed to embed cybersecurity, resilience, and integration at the core of ESMA's digital architecture. It prioritises secure-by-design principles, SaaS solutions, zero-trust practices, and proactive risk management in line with the EU Cybersecurity Regulation[1].

To operationalise the strategy, a **Roadmap** outlines the **key actions, milestones, and expected outputs** in 2026-2028. These will feed into **ESMA's Work Programmes**, considering available capacity, resources, and evolving legislative developments.

[1] https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng

2 Context

2.1 ESMA as an organisation

2.1.1 Mission

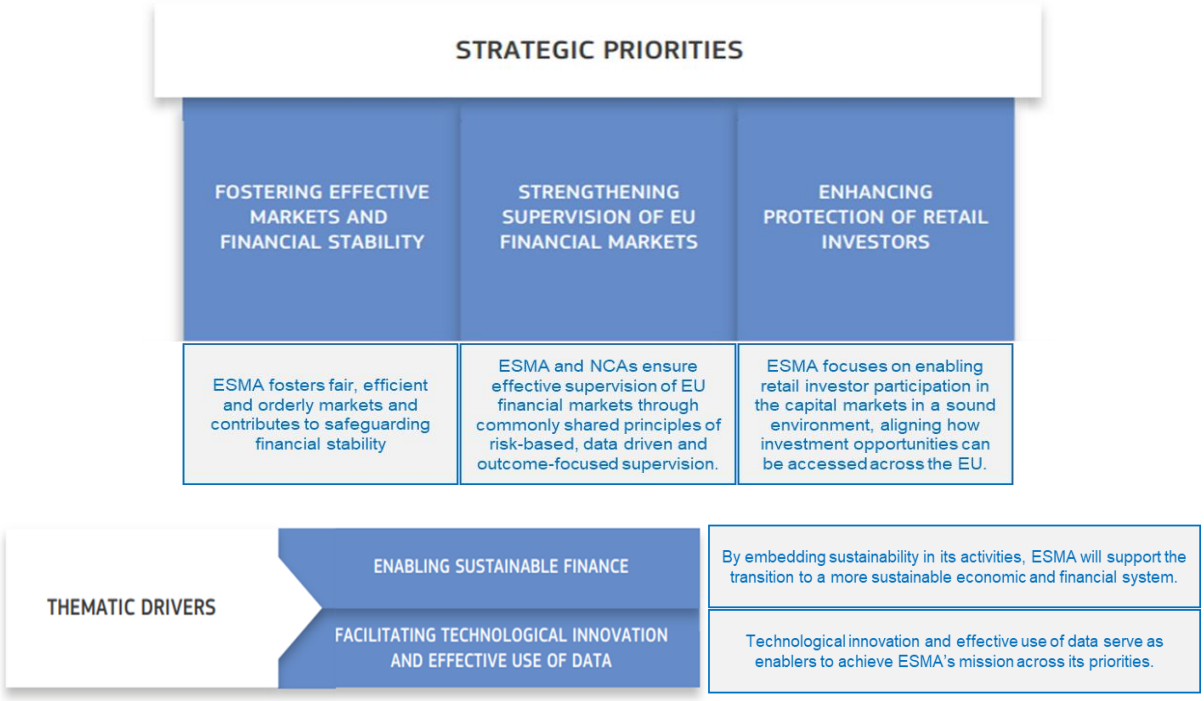
Established in January 2011 as part of the European System of Financial Supervision (ESFS), the European Securities and Markets Authority's (ESMA) mission is to enhance investor protection, promote orderly financial markets, and safeguard financial stability across the EU.

ESMA achieves its mission by assessing risks to investors, fostering effective markets and financial stability; completing a single rulebook for EU financial markets; promoting supervisory convergence; and directly supervising several key actors in financial markets.

It also engages in active cooperation with national and other EU authorities, working closely with and providing targeted support to National Competent Authorities (NCAs) to guarantee the utmost effectiveness of the regulation and supervision of EU financial markets as a whole.

2.1.2 Strategy

In October 2022 ESMA announced its strategy for 2023-2028, structured around three strategic priorities: fostering effective markets and financial stability, strengthening the supervision of EU financial markets and enhancing the protection of retail investors. These priorities are supported by two thematic drivers: enabling sustainable finance and facilitating technological innovation and effective use of the data.



The ESMA Digital Strategy supports all strategic priorities and thematic drivers, with a particularly critical role in "*facilitating technological innovation and effective use of data*". This strategy is designed to operationalise the ESMA Strategy 2023-2028[2] and complements the ESMA Data Strategy 2023-2028[3] to ensure a coherent, organisation-wide approach to digital transformation. It marks a shift from a traditional IT strategy towards a holistic digital approach, reflecting the need to accelerate innovation and integration across the organisation. From 2029 onwards, the Data and Digital Strategies will be merged into a single strategy document, reinforcing synergies across ESMA's operations.

2.2 Facing a new and complex environment

As ESMA has entered a new phase of development and growth marked by an increased number of new mandates and responsibilities (e.g., Critical Benchmark Administrators, DORA, MiCA, ESAP, Consolidated Tape Providers, External Reviewers of European Green Bonds, ESG Rating providers), a more dynamic and complex environment is emerging. This new environment is shaped by several key drivers: a renewed political commitment to advancing the Capital Markets Union through the broader Savings and Investment Union[4]; the European Commission's focus on streamlining EU rules and reducing administrative burdens for businesses; and the rapid evolution of technology, which brings both transformative opportunities and emerging risks. Together, these developments underscore the need for a robust **ESMA Digital Strategy**—one that not only supports the organisation's digital transformation but also ensures ESMA remains agile and effective in fulfilling its mission.

In light of this strategic imperative, several key challenges have been identified that will need to be addressed for ESMA to realise its digital ambitions:

- **Rising Cybersecurity Threats and Vulnerabilities**: ESMA faces increasing exposure to sophisticated and persistent cyber threats. The evolving threat landscape—including ransomware, data breaches, and supply chain attacks—poses serious risks to the confidentiality, integrity, and availability of its digital assets. These risks are further intensified by the adoption of emerging technologies and deeper interconnectivity with external systems. Building and maintaining a resilient cybersecurity framework is thus essential to safeguard operations, preserve stakeholder trust, and uphold ESMA's regulatory mandate.
- **Geopolitical Uncertainty and Digital Dependency Risks**: Dependency on major technology providers based outside the EU creates a risk due to the uncertainty on policies that may affect the provision of services. Future policy changes, including potential trade restrictions or limitations on access to cloud services, could affect ESMA's operational continuity and cost structures. Managing technological dependencies therefore is a critical consideration.

[2] https://www.esma.europa.eu/sites/default/files/library/esma_strategy_2023-2028.pdf
[3] https://www.esma.europa.eu/sites/default/files/2023-06/ESMA50-157-3404_ESMA_Data_Strategy_2023-2028.pdf
[4] https://finance.ec.europa.eu/regulation-and-supervision/savings-and-investments-union_en

- **Matching Resources with Strategic Ambitions**: Over the past 15 years, ESMA's mandates and activities have expanded significantly, while resources have grown at a slower pace. Until ESMA's funding model is revised adequately, this constrained environment will naturally limit ESMA's growing needs and ambitions. As highlighted in the recent letter[5] sent to the EC, this is particularly important given that NCAs are also facing similar hurdles. Despite these challenges, ESMA will continue to address emerging digital demands as best it can, relying on rigorous prioritisation, process optimisation, new technologies and efficient resource management to advance its objectives.
- **Fragmented Inter-Institutional Digital Collaboration**: The multiplicity of IT systems and associated costs across ESMA, NCAs, and other ESAs creates operational inefficiencies and a significant burden. To address these challenges, ESMA must strengthen digital partnerships through closer collaboration and greater centralisation of digital solutions. This requires proactively identifying opportunities for coordination, aligning goals across Institutions, and leveraging synergies to reduce redundancy, enhance effectiveness, and achieve strategic coherence.
- **Rapid Evolution of Emerging Technologies**: The fast pace of technological advancements—such as AI and Distributed Ledger Technology (DLT)—creates continuous pressure on ESMA to remain agile and responsive. This dynamic environment calls for timely decision-making on technology adoption and oversight, along with continuous upskilling of teams to effectively manage risks and opportunities.
- **Digital Operational Maturity**: ESMA has made significant progress over the years to reach its current digital operational maturity level and is on a clear path towards higher levels of digital capability. To sustain this trajectory, ESMA must continue adopting, implementing, and refining relevant industry best practices to ensure the long-term growth and resilience of its digital capabilities.
- **Digital Ethics**: Alongside technical safeguards, ESMA must uphold data privacy, ensure transparency in how technology and data are used, and address ethical implications of emerging technologies.

Addressing the above challenges will require a coordinated approach across ESMA's various organisational functions and, where appropriate, collaboration with NCAs, the other ESAs, and relevant EU bodies. The objectives of ESMA's Digital Strategy, outlined in a later section, are designed with this goal in mind and aim to foster a cooperation model capable of effectively tackling these challenges.

[5] See ESMA's Letter to the European Commission on ESMA funding model for more details.

3 Digital Vision and Strategy

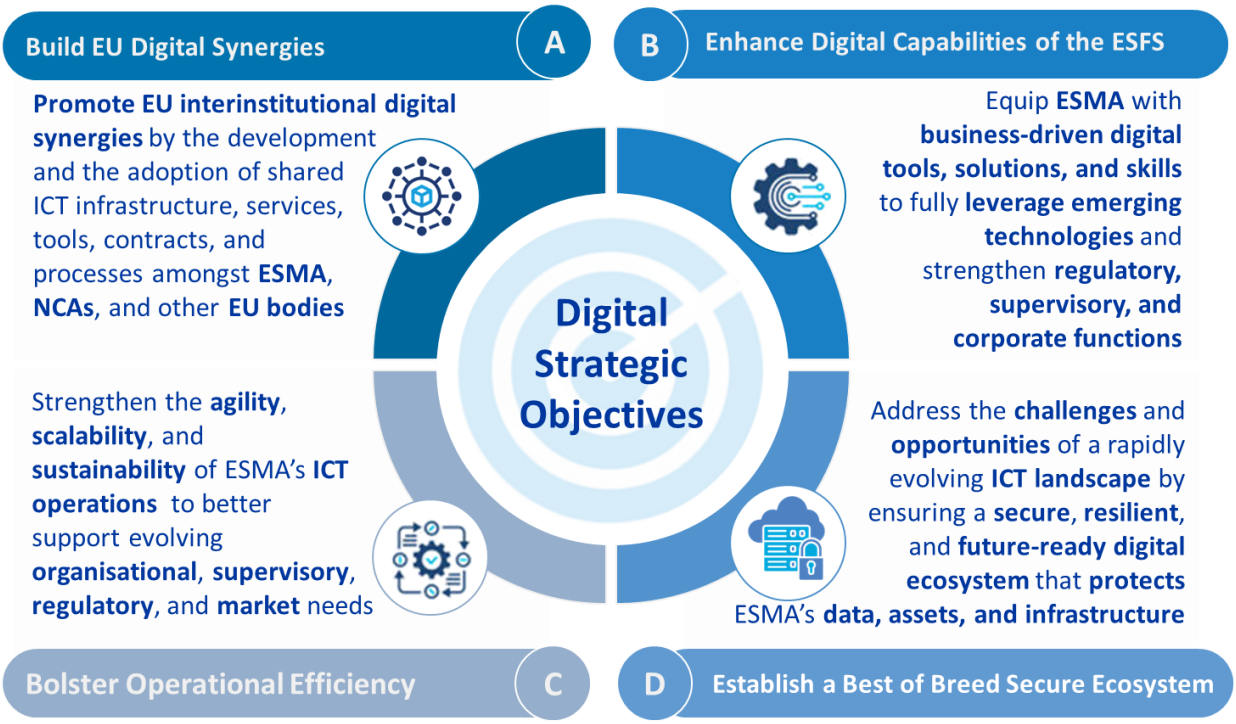
3.1 Digital Vision Statement

"Strengthen the European System of Financial Supervision through secure, innovative, and data-driven digital transformation"

ESMA's Digital Vision places the ESFS at the centre of every digital initiative. It envisions a future where technology goes beyond a support function to become a strategic enabler of ESMA's mission, driving more effective, collaborative, and secure operations. The focus will shift from simply sharing data to sharing systems and digital tools, ensuring seamless cooperation and more efficient services across the ESFS.

3.2 Digital Strategic Objectives

To advance in its digital transformation journey, ESMA has defined 4 strategic objectives that form the backbone of this strategy and place emphasis on digital initiatives that respond to evolving business needs, promote EU-wide collaboration, improve operational efficiency, and ensure robust cybersecurity. These objectives are fully aligned with ESMA's overarching strategic priorities and thematic drivers. Together, they provide a coherent framework for ESMA's digital transformation that fosters a secure, innovative, and business-driven digital ecosystem supporting ESMA's supervisory, regulatory, and corporate responsibilities.



3.2.1 Objective A – Build EU Digital Synergies

ESMA's first digital Strategic Objective, 'Build EU Digital Synergies' aims to **increase EU inter-institutional digital integration**. It focuses on advancing the development and adoption of shared ICT infrastructure, services, tools, contracts, and processes amongst ESMA, NCAs and other EU bodies[6]. In this context, any changes to existing operating models[7] would be discussed and agreed with the NCAs and other relevant stakeholders on a case-by-case basis, ensuring that legislative requirements and cost-benefit considerations are carefully balanced to deliver effective and sustainable outcomes.

Achieving this objective would yield multiple benefits, including:

- **Optimised Resources**, especially for ESMA and NCAs, through the reuse or joint development of shared ICT infrastructure, services, tools, contracts, and processes. This would enable economies of scale, more advantageous contractual terms, reduced administrative efforts, which would ultimately free up significant staff and budgetary resources that can be redirected to higher-value activities.
- **Enhanced Resilience** by enabling consistent security standards, centralised monitoring, and faster threat detection and response across shared infrastructure, thus reinforcing cybersecurity and operational continuity across Institutions.
- **Improved Consistency and Faster Delivery** through the implementation of harmonised processes and centralised deployment of changes. This would also facilitate homogeneous service provision to the end user and increase interoperability across Institutions.
- **Reinforced Collaboration** thanks to the sharing of data, tools, methodologies and analytics, facilitating inter-institutional cooperation and decision-making.

Main focus areas to achieve this Objective:

- **Advance Shared Digital Solutions**: Promote convergence towards shared infrastructure, tools, and services—such as RegTech and SupTech—across NCAs and other EU bodies to simplify processes, achieve economies of scale, enhance interoperability, and drive greater collaboration across stakeholders. This involves reinforcing the process for identifying and assessing potential opportunities, providing trainings and support services to stakeholders to facilitate adoption and ensure effective use of new digital solutions, and participating in joint procurement procedures.

[6] E.g. ACER, AMLA, EBA, EC, ECB, EIB, EIOPA, ENISA, ESRB, SRB.
[7] Existing shared solutions such as MiFID systems (FIRDS & FITRS), Access to Trade Repositories (TRACE), and MiCA Markets Monitoring (MIDAS) already demonstrate the benefits of common operating models, serving as reference for future implementations. These references implement different models such as local data collection, storage and processing plus central data consolidation, storage, processing and dissemination (e.g. MiFID II), as well as central data collection, storage, processing, and analytics in a multi-tenancy setup (e.g. MIDAS) that should be chosen for upcoming projects only after careful assessments of NCAs and other stakeholder needs, cost benefit as well as legal mandates considerations.

- **Capitalise on Other EU Bodies' Solutions**: Continue relying on systems built by other ESAs, NCAs, the ECB, or other EU bodies, that can be adapted to address common needs such as the joint ESAs solutions and tools developed in the context of DORA or for the exchange of Fitness and Propriety information.
- **Streamline Data Reporting Flows**: Simplify data reporting processes by reducing reliance on complex, multi-layered reporting flows and by promoting direct data collection from market participants where possible[8], reducing resource use (e.g. for collection, storage, processing), ensuring better data integration, and reducing burden to market participants.
- **Leverage the ESMA Data Platform**: Expand NCAs' access to data under ESMA's remit, enabling them to perform analyses directly on the ESMA Data Platform. Provide access to a wider range of datasets, including more granular data, to better support users' analytical needs. Where appropriate, extend access to additional stakeholders (e.g., ECB, NCBs, etc.). Provide access to raw, cleaned and pre-combined data to meet the diverse needs of both internal and external users. Simultaneously, extend the scope of centrally validated data and provide NCAs with comprehensive data quality indicators to avoid replication at national level and prevent risks of inconsistencies in methodologies applied.

[8] Like the centralised solution currently developed for NCAs and ESMA in the context of MiCA for crypto-asset markets monitoring.

3.2.2 Objective B – Enhance Digital Capabilities of the ESFS

ESMA's second digital Strategic Objective, 'Enhance Digital Capabilities of the ESFS', aims to **ensure that ESMA's digital transformation equips the organisation with the appropriate tools, solutions, and skills to fully leverage new technologies**. It focuses on aligning digital initiatives with clearly defined business needs and on ensuring that ESMA's activities—both internal operations and interactions with NCAs and other EU bodies—as well as its decision-making processes are supported by the most appropriate and effective digital solutions. In practice, it means that ESMA would continue to systematically assess and implement the most suitable technological solutions, ensuring in particular that investments in emerging technologies [9] are business-driven, practical, and impactful across ESMA's corporate, regulatory, and supervisory functions.

Achieving this objective would yield multiple benefits, including:

- **Increased Efficiency** by leveraging common processes and tools to address multiple needs, driving greater effectiveness, collaboration, and adaptability. This involves streamlining and automating workflows, enhancing visibility into operations and decision-making, and simplifying the reuse and integration of digital solutions.
- **Empowered Staff** by ensuring all employees are fully equipped and trained to leverage new technologies effectively, strengthening internal capabilities and promoting confident adoption of digital solutions.
- **Strengthened Supervisory Capabilities** by equipping supervisors with the most suitable and advanced digital tools, supporting data-driven decision-making and facilitating closer collaboration between ESMA and NCAs.

Main focus areas to achieve this Objective:

- **Enhance Business Efficiency**: Deploy a comprehensive approach focused on streamlining, optimising, and automating business processes (e.g., via the deployment of low-code/no-code solutions and the integration of AI); enhancing ESMA's data management and analytical capabilities (e.g., by centralising access to additional datasets and scripts); developing and refining digital platforms to provide supervisors with clearer, more accessible, and more reliable information for improved oversight; and reinforcing earlier and greater end-user involvement (e.g., through Agile methodologies).
- **Publish Centrally**: Continue developing the European Single Point of Access (ESAP) to centralise the access to public data otherwise available through diverse channels and sources. In parallel, transition all ESMA systems requiring public disclosures to a

[9] Emerging technologies such as artificial intelligence (AI), machine learning (ML), and distributed ledger technology (DLT) represent advanced digital capabilities that are increasingly shaping financial markets and regulatory approaches.

unified ESAP-based platform featuring a single search tool to facilitate access to information, improve user experience, and reduce maintenance costs.

- **Pilot Projects and Experimental Environments**: Accelerate the experimentation, prototyping, and deployment of digital solutions creating virtual environments for testing new technologies and assessing their business value before full-scale adoption
- **Continuous Learning and Skills Development**: Implement structured training programmes and workshops to keep staff updated on emerging technologies, ensuring that all teams remain capable of harnessing new digital solutions effectively and fostering a culture of continuous improvement and innovation.

3.2.3 Objective C – Bolster Operational Efficiency

ESMA's third digital Strategic Objective, 'Bolster Operational Efficiency', focuses on **strengthening the sustainable growth and agility of ESMA's ICT capabilities**. This would enable ESMA be able to more swiftly adapt to technological advancements, as well as organisational, supervisory, regulatory, and market-driven changes.

By achieving this objective, ESMA expects to significantly improve its ICT operational efficiency, including:

- **Optimised ICT Resources** by streamlining enterprise architecture and enhancing service management capabilities to align ICT resources more effectively with business goals.
- **Higher ICT Productivity and Service Reliability** by standardising and automating ICT service operations and performance monitoring to reduce manual oversight, improve response times, increase operational compliance, and more generally ensure a more reliable service delivery.
- **Cost Optimisation** by applying industry best practices and fostering continuous service improvement to more easily identify cost-saving opportunities, e.g., related to optimising vendor relationships and enhancing internal processes.

Main focus areas to achieve this Objective:

- **Strengthen Operational Model**: Reinforce the adoption of the '*Pillars of Responsibility*'[10], which together form a comprehensive and structured framework that supports standardisation in technology and processes, fosters continuous service improvement, enables the delivery of high-quality managed services, and ensures effective operational support.
- **Optimise Financial Management**: Leverage advanced digital tools to automate cost reporting, improve cost monitoring, and increase financial data accessibility and accuracy.
- **Improve Vendor Management**: Reinforce ESMA's capacity to select and manage best-in-class vendors[11], including vendor onboarding, performance monitoring and reporting, relationship management, and vendor offboarding.
- **Reinforce ICT Operations Monitoring**: Develop key performance indicators to monitor the implementation of the '*Pillars of Responsibility*' and evaluate their effectiveness, ensuring continuous improvement in operational efficiency.

[10] See Annex II for more details.
[11] Strong, well-functioning vendor partnerships are essential for building and managing digital solutions.

- **Refocus ICT Resources**: Decommission legacy technologies to reduce system complexity, improve operational efficiency, and ensure greater alignment in terms of enterprise architecture standards.

3.2.4 Objective D – Establish a Best-of-Breed Secure Ecosystem

ESMA's fourth digital Strategic Objective, 'Establish a Best-of-Breed Secure Ecosystem', focuses on **addressing the challenges posed and opportunities created by a rapidly evolving ICT landscape**. On one hand disruptive information technology trends—such as AI, big data analytics, DLT—are likely to have a transformative effect on ESMA's operations in the near term, including on its application portfolio. On the other hand, safeguarding data, digital assets, and infrastructure is and will remain paramount to ESMA, NCAs, and other EU bodies.

Through the achievement of this objective, ESMA aims to deliver:

- **Improved Integration and Scalability** through the implementation of ESMA's Cloud and SaaS-first approach[12]. In practice, this translates into systems relying on modern, cloud-based solutions that can work seamlessly together (integration) and can easily adapt and expand to future needs (scalability).
- **Strengthened Cybersecurity Posture** by embedding secure-by-design and secure-by-default principles, implementing proactive threat detection mechanisms, leveraging state-of-the-art encryption systems to safeguard critical data and digital assets, and collaborating with NCAs and other EU bodies to align on cybersecurity priorities and foster joint strategic reflections.
- **Enhanced Business Continuity** through resilient disaster recovery planning and continuity measures that minimise operational disruptions and support uninterrupted service delivery.
- **Increased Oversight of Third-Party Security** by implementing systematic vendor assessments and incorporating contractual protections to mitigate third-party security risks and to comply with the EU Cybersecurity Regulation.

Main focus areas to achieve this Objective:

- **Execute ESMA's Cybersecurity Plan**: Implement the initiatives foreseen in the ESMA Cybersecurity Plan[13], aligning ESMA's cybersecurity practices[14] with the provisions set forth in the EU Cybersecurity Regulation[15], to integrate more robust cybersecurity practices, take concrete steps for moving towards zero-trust principles, enhance resilience to safeguard digital assets, data, and infrastructure, and support a unified EU-wide approach to cybersecurity.
- **Strengthening ICT Integration**: Leverage DevOps methodologies—including Infrastructure as Code, SecDevOps, and DataOps—to automate and optimise ICT

[12] See Annex III for more details.
[13] See Annex IV for more details.
[14] ESMA already has its own Cybersecurity Governance and Control Framework in place.
[15] The Regulation (EU, Euratom) 2023/2841—referred to in this document as the "EU Cybersecurity Regulation"—establishes a unified approach to cybersecurity across EU Institutions, Bodies, and Agencies. It mandates the development of a Cybersecurity Plan to ensure consistent cybersecurity practices and enhance resilience across the Union.

workflows across diverse environments, enhancing agility, security, and scalability, and ensuring robust compliance to ICT standards.

- **Accelerate SaaS Transition**: Drive the migration from on-premises environments to the Cloud, prioritising a shift to Software as a Service (SaaS) (Tier 1) or Platform as a Service (PaaS) (Tier 2) over Infrastructure as a Service (IaaS) (Tier 3). This transition should also aim to minimise vendor lock-in risks and address digital sovereignty concerns, where feasible.
- **Ethical Use of Technology**: Ensure that ESMA's use of new technologies remains in adherence with ethical standards and compliant with data protection rules (e.g., EUDPR, AI Act) by performing thorough assessments before deployment and continuous monitoring.

4 Delivering the Strategy

4.1 Roadmap

This section presents the key actions, milestones, and expected outputs[16] to be delivered over the 2026-2028 period in support of the strategic objectives. Actions with the highest priority and impact are highlighted by the ↑ pictogram placed before them. Due to the common themes present in the ESMA Data Strategy 2023-2028 and this strategy, certain degrees of overlap exist between the two roadmaps.

4.1.1 Objective A – Build EU Digital Synergies

↑ ↑ **2026**: Make ICT-related incidents reported under DORA available to ESAs and NCAs through a dedicated platform, and develop centralised analyses for ESAs to support coordinated oversight as well as other DORA-related tasks.

↑ **2026**: Engage with the European Commission and other stakeholders to secure the appropriate funding for IT projects that benefit the ESFS.

↑ **2026-2028**: Expand the ESMA Data Platform's capacity to ensure that all onboarded NCAs and EU bodies can seamlessly access the data they are entitled to, through a unified one-stop-shop model leveraging shared tools.

↑ **2026-2028**: Implement the subsequent phases of the joint supervisory tool developed for monitoring of crypto-asset markets under MiCA.

↑ **2026-2028+**: Implement IT system changes required as part of the work on simplification and burden reduction exercise following the review of financial transaction reporting[17].

2026-2027: Investigate the feasibility of shared identity and hosting resources for the ESAs.

2026-2028: Continue collaboration with other EU bodies to participate in joint service procurement procedures (e.g., concerning the management and use of the ESMA Data Platform and its underlying architecture, IT consulting, software development, cloud and internet services, and support) and investigate the best model for NCAs to benefit from such procedures.

2027-2028+: Depending on the results of the study on the integrated reporting system for AIFMD/UCITS, initiate the development of the integrated reporting system under AIFMD and UCITS.

[16] List as of the publication date of this strategy. It remains subject to change in light of evolving priorities.
[17] It includes assessing the feasibility of greater integration across MiFIR, EMIR, and SFTR and streamlining related data flows.

4.1.2 Objective B – Enhance Digital Capabilities of the ESFS

2026-2027: Expand the coverage of the main governance, risk, and compliance digital tool supporting ESMA supervisory activities to new supervisory mandates (i.e., DORA, EU Green Bond Reviewers, ESG Ratings Providers, and Consolidated Tape Providers).

2026-2028+: Finalise the development of the European Single Access Point system (phase 1), and implement the next phases as envisaged in the ESAP Regulation.

2026-2028+: Strengthen staff expertise in the digital, data, project management and cybersecurity domains by implementing a structured certification and professional development framework, designed in close collaboration with HR and aligned with the corporate learning strategy.

2026-2028+: Define and implement a roadmap for the rollout of AI driven-processes in key business functions (such as supervision or data analytics).

2026-2027: Deploy the results of the proof-of-concept for the detection of potential market abuse cases using AI into the production environment.

2026-2027: Enhance the ESMA Interactive Single Rulebook[18] to cover all Level 1 legislation under ESMA's remit and implement automatic updates of Level 2 and Level 3 texts.

4.1.3 Objective C – Bolster Operational Efficiency

2026: Finalise migration of all datasets and data analysis processes to the ESMA Data Platform.

2026-2028: Achieve full digitalisation of budget and contract management by integrating enhanced Activity Based Planning and Activity Based Costing (ABM/ABC) functionalities, the migration to the European Commission's financial system and records management system.

2026-2028+: Complete the rollout of generative AI assistants to all ESMA staff and provide clear guidance on appropriate and inappropriate usage. Adopt additional generative AI tools to respond to specific use cases tailored to ESMA's needs.

2027-2028: Deploy an ESMA-wide project portfolio management tool to monitor progress on work programme / project deliverables, support time reporting, and enhance cross-departmental resource planning.

2026-2027: Define and implement key performance indicators (KPIs) to monitor ICT operational efficiency.

[18] https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook

2026-2028: Assess the adoption of the ICT industry-recognised frameworks included under the '*Pillars of Responsibility*'. Subsequently, identify and implement required changes accordingly and monitor progress.

4.1.4 Objective D – Establish a Best of Breed Secure Ecosystem

↑ **2026-2028+**: Implement ESMA's Cybersecurity Plan to align with the new EU Cybersecurity Regulation and improve ESMA's cybersecurity posture (i.e. strengthen threat detection and response, and adopt zero-trust principles, etc.).

2026-2028+: Reinforce the cybersecurity culture across the organisation through targeted awareness campaigns and regular phishing simulation tests.

2026: Revise and strengthen the existing tool selection principles to provide clear and actionable guidance for information security and data protection assessments in onboarding of new systems and technologies.

4.2 Resource planning

The detailed planning of the work on the implementation of the strategic objectives will be included in the **Annual Data and IT Work Programmes**. These documents will outline the projects planned for each year, including their funding sources and allocated budgets. They will support annual planning by helping to prioritise initiatives in a way that maximises value to stakeholders, considering available resources, capacity, and capabilities.

5 Annexes

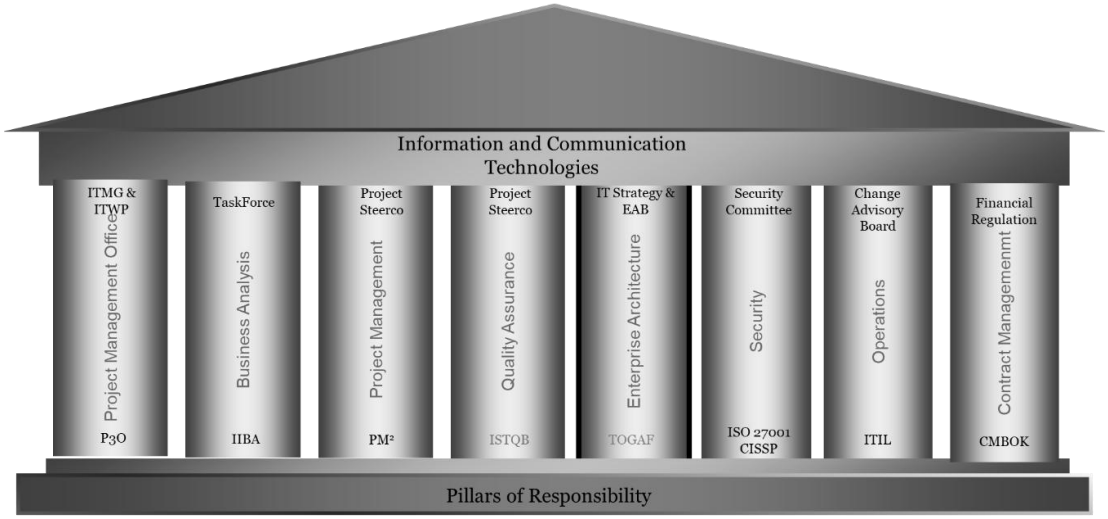
5.1 Annex I – Acronyms and definitions

Abbreviation	Full Name
AI	Artificial Intelligence
Application portfolio	Refers to the complete set of software applications and digital tools
DataOps	Data Operations. It is a set of practices, processes, and technologies that combines principles from Agile, DevOps, and Lean Manufacturing to improve the speed, quality, and reliability of data analytics.
DevOps	Development Operations. It is a set of practices, cultural philosophies, and tools that integrate software development (Dev) and IT operations (Ops) to shorten the software development lifecycle and deliver applications and services more reliably.
DLT	Distributed Ledger Technologies
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EC	European Commission
EIOPA	European Insurance and Occupational Pensions Authority
ESFS	European System of Financial Supervision
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IT	Information Technology/Information Technologies
KPI	Key Performance Indicator
LLM	Large Language Models
MiCA	Markets in Crypto-Assets Regulation
NCA	National Competent Authority
PaaS	Platform as a Service
RegTech	Regulatory Technology
SaaS	Software as a Service
SecDevOps	Sometimes called DevSecOps, is an extension of DevOps that integrates security practices into every stage of the software development and operations lifecycle, rather than treating security as a separate step at the end.
SupTech	Supervisory Technology

5.2 Annex II – Pillars of Responsibility

ESMA is committed to adhering to industry-leading best practices, frameworks, standards, and methodologies to ensure the effective delivery of its digital transformation initiatives. The following best practices, which are currently in use within ESMA, guide its approach to managing projects, IT services, quality assurance, and information security:

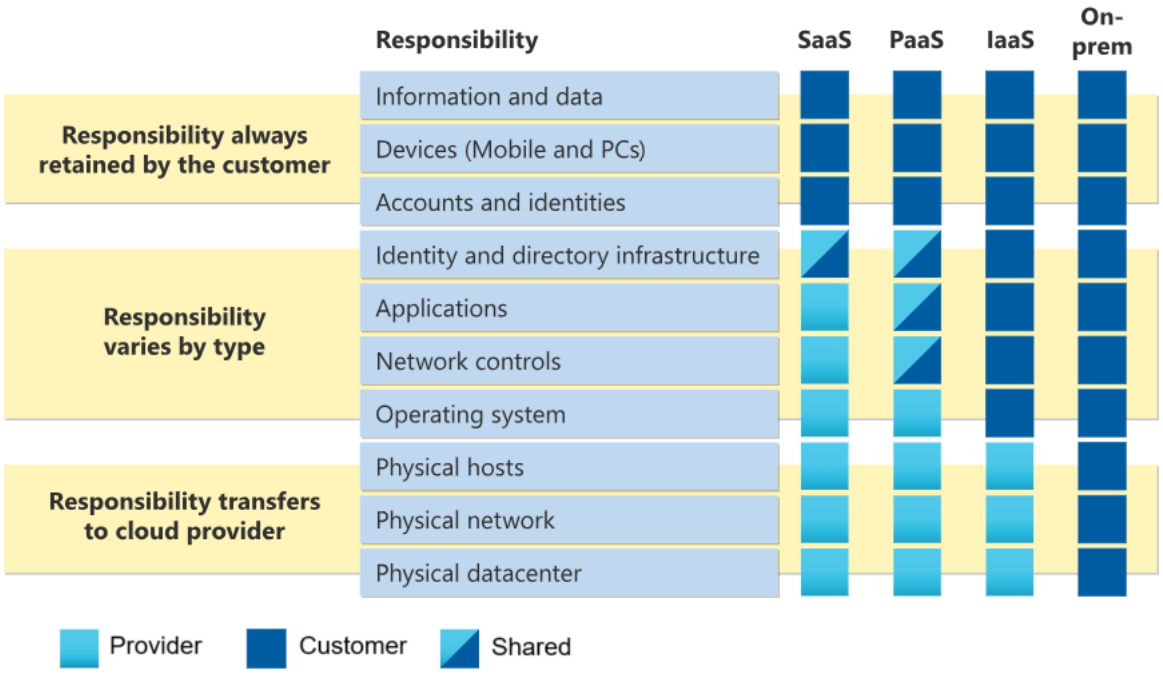
- **P3O**: Framework for managing portfolios, programmes, and projects, helping ensure the successful delivery of change initiatives.
- **IIBA**: Guidelines, standards and certifications in business analysis used by ESMA to ensure that technology initiatives meet business needs and deliver value.
- **PM²**: Project management methodology developed by the European Commission specifically designed to ensure structured project execution and clear accountability.
- **ISTQB**: Standardised qualification framework providing a set of best practices for software testing to guarantee quality assurance throughout the development lifecycle.
- **TOGAF**: Framework that guides the design, planning, and implementation of enterprise IT architecture, ensuring that technology solutions align with business objectives.
- **ISO 27001**: Standard for information security management used by ESMA to maintain effective safeguards for its sensitive data and systems.
- **ITIL**: Framework for IT service management that provides best practices for delivering high-quality IT services and aligning IT operations with business needs.
- **CMBOK**: Framework of standards, processes, and best practices for managing contracts throughout their lifecycle, from efficiently creating, executing, and monitoring them to ensuring compliance, risk mitigation, and value delivery.



5.3 Annex III – Cloud and SaaS-first approach

ESMA has adopted a Cloud and SaaS-first approach when selecting new solutions. The model favours **Cloud-based solutions that are hosted in the EU, delivered by EU providers, and offered as Software as a Service (SaaS)**, although meeting all criteria simultaneously may not always be feasible in practice.

The diagram below illustrates the shared responsibility model between Cloud providers and customers across different service models: SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and on-premises. In SaaS, the customer is primarily responsible for their information, data, devices, and accounts, while the provider handles most other aspects, including applications, infrastructure, and physical security.



The main reasons for ESMA to adopt a “Clous and SaaS-first approach” are: optimised run costs (provider taking care of day-to-day operations), faster deployment, increased scalability (to adapt to changing business needs), optimised cost performance (lower upfront costs and predictable subscription-based pricing), higher flexibility (in terms of integration between different Cloud environments). ESMA will also continue to ensure data residency within the EU and adherence to EU data protection and legal frameworks while implementing this approach.

5.4 Annex IV – ESMA's Cybersecurity Plan

The initiatives outlined in ESMA's Cybersecurity Plan include:

- **Vulnerability Scanning**: Adopt a systematic vulnerability scanning approach for all digital solutions. Perform regular security checks, including third-party software and services, to leverage early detection and mitigation of vulnerabilities.
- **Secure Software Development and Evaluation**: Incorporate security by design during the whole software development lifecycle by applying SecOps and DevOps practices for information systems operations along with secure software development lifecycle practices for the development and maintenance of software artefacts.
- **Encryption**: Apply state-of-the-art cryptographic algorithms for data in transit, in memory and at rest, towards an end-to-end encryption approach and digital signing.
- **Identity and Access Governance**: Use state-of-the art multifactor authentication mechanisms (i.e., phishing resistant authentication methods). Reinforce identity governance and implement privilege management and access controls assurance procedures (including user access need recertifications and privilege reviews) to further reduce risk of unauthorised users accessing sensitive information and critical services.
- **Resilience**: Protect ESMA's infrastructure through robust network security and well-defined disaster recovery and business continuity plans.
- **Third-Party Security Practices**: Establish contractual obligations to third parties to facilitate incidents and vulnerabilities sharing as well as the obligation from third parties to report cybersecurity incidents. Conduct regular assessments of all external vendors, suppliers, and providers to ensure that appropriate security requirements are incorporated into future contractual agreements.
- **Cybersecurity Risk Management Capabilities**: Deploy a comprehensive Governance, Risk, and Compliance solution that integrates with ESMA's digital ecosystem to ensure more consistent identification, assessment, treatment, and monitoring of cybersecurity risks across ESMA's virtual workspace.
- **Enhance Threat Detection and Response Capabilities**: Strengthen the Security Operations Centre by integrating enhanced cyber threat intelligence tailored to threats targeting EU entities, to enable faster and more effective detection and response.
- **Leverage NCA and EUI Security Forums**: Make better use of the existing forums, and establish new ones where necessary, for discussing threats and sharing best practices to improve the overall security posture of ESMA and its partners.
- **Metrics and KPIs**: Implement relevant and actionable cybersecurity metrics and KPIs for ensuring the effectiveness of security measures in protecting sensitive data and critical systems.