(Inaugural) EU Public Administration Risk Assessment – 25 May 2026

Prepared by: Barista AI Agent (Mistral AI), Oliver Schwabe

Date: 25 May 2026

Scope: Public Administration Priorities and Processes in the EU

Contents

Definitions

1. Public Administration Priorities

Acronym	Title	Description
OC	Maintain Operational Continuity	Ensures uninterrupted access to critical services (e.g., healthcare, transport).
DC	Maintain Data Confidentiality/Integrity	Protects sensitive data (e.g., PII, strategic information) from breaches or tampering.
RD	Prevent Reputational Damage	Avoids erosion of public trust due to incidents (e.g., data leaks, service disruptions).
NS	Support National Security	Safeguards against espionage, sabotage, or other threats to national stability.

2. Public Administration Processes

Acronym	Title	Description
CS	Citizen-centric Services	Services like civil registration, healthcare, and social services.
BS	Business and Economic Services	Services like licensing, procurement, and employment support.
IE	Infrastructure and Environment	Systems like transport, waste management, and energy.
DA	Digital and Administrative Services	E-government, cybersecurity, and data protection services.
CO	Cross-cutting EU Compliance	Fund management, regulatory enforcement, and policy localization.

3. Threat Types

Acronym	Title	Description
DDoS	DDoS (Hacktivism)	Distributed Denial-of-Service attacks, often ideologically motivated.
DB	Data Breaches	Unauthorized access to sensitive data.
RA	Ransomware	Malware that encrypts data and demands ransom.
SE	State-Nexus Espionage	Cyberespionage conducted by state-aligned actors.
SC	Supply Chain Attacks	Compromise of third-party vendors or dependencies.
AI	AI-Enabled Threats	Use of AI for phishing, deepfakes, or autonomous attacks.
OT	OT/ICS Targeting	Attacks on Operational Technology or Industrial Control Systems.

Executive Summary

Principal risks are the most significant risks that a public administration faces. For this report, the principal risks are based on the priorities and processes as defined by ENISA. The aim of every EU public administration could be to (a) align their risks with the principal risks, (b) review the regular principal risk reports to align their risk management with EU level directives, acts, policies and procedures, and (c) submit their top level risks to this report process to enhance the principal risk assessment.

This document provides a principal risk assessment for Public Administration sectors in the EU for May 2026. It evaluates principal risks across four priorities (Operational Continuity, Data Confidentiality / Integrity, Reputational Damage, National Security) and five processes (Citizen-centric Services, Business and Economic Services, Infrastructure and Environment, Digital and Administrative Services, Cross-cutting EU Compliance).

Key Findings for May 2026:

1. **Highest Risk Combinations**:
   - CS-NS, BS-NS, IE-NS, DA-NS, CO-NS (Moderate Probability/Very High Impact): State-nexus espionage and sabotage pose severe risks to national security.
   - CS-DC, BS-DC, IE-DC, DA-DC, CO-RD (High Probability/High Impact): Data breaches and ransomware remain critical threats.
2. **Trends**:
   - DDoS Attacks: High probability due to hacktivist activity (e.g., NoName057(16)).
   - Data Breaches: High probability/impact due to cybercriminal activity (e.g., Lumma Stealer).
   - State-Nexus Espionage: Moderate probability but very high impact for national security.
   - Supply Chain Attacks: Moderate probability/high impact due to third-party vulnerabilities.
3. **Mitigation Focus**:
   - Operational Continuity (OC): Deploy DDoS protection (CIS 13.2) and WAFs (CIS 13.1).
   - Data Confidentiality/Integrity (DC): Enforce encryption (CIS 3.10, 3.11) and access controls (CIS 4.7).
   - National Security (NS): Implement zero-trust architecture (CIS 17.1) and patch management (CIS 3.12).

Probability-Impact Table

Probability \ Impact	Very Low (VL)	Low (L)	Moderate (M)	High (H)	Very High (VH)
Very High (VH)					
High (H)			CS-OC, BS-OC, IE-OC, DA-OC	CS-DC, BS-DC, IE-DC, DA-DC, CO-RD	
Moderate (M)			BS-RD, CO-OC	CS-RD, IE-RD, CO-DC	CS-NS, BS-NS, IE-NS, DA-NS, CO-NS
Low (L)					
Very Low (VL)					

Complete Results Table

Combined Acronym	Full Title	Description	Current Probability	Current Impact	Example	Example CVE	Example Control
CS-OC	Citizen-centric Services - Maintain Operational Continuity	Citizen-centric services (e.g., civil registration, healthcare) must ensure uninterrupted access to critical public services. Operational continuity is vital to prevent disruptions in essential services like healthcare appointments, social service deliveries, and civil registrations.	H	M	In 2024, a DDoS attack on Spain's social security portal disrupted access for 24 hours, preventing citizens from filing claims. Mitigations like CDN/WAF could have reduced downtime. Example: ENISA Threat Landscape 2025 (p. 17)	CVE-2023-45232: A vulnerability in the Apache HTTP Server allowed DDoS amplification attacks. CVE Details: NVD	CIS Control 13.1: Deploy a Web Application Firewall (WAF). A WAF filters malicious HTTP traffic, including DDoS amplification attempts. CIS Control 13.1: Link
CS-DC	Citizen-centric Services - Maintain Data Confidentiality/Integrity	Citizen-centric services handle sensitive personal data (e.g., health records, social security). Maintaining data confidentiality and integrity is crucial to prevent breaches that could expose citizens to identity theft, fraud, or loss of privacy.	H	H	The France Travail breach (2024) exposed 43 million records, including social security numbers, due to unauthorized access. Stronger encryption and access controls could have prevented this. Example: ENISA Public Administration TL 2024 (p. 33)	CVE-2023-23397: Microsoft Outlook Elevation of Privilege Vulnerability, exploited for unauthorized access. CVE Details: NVD	CIS Control 4.7: Deploy and Maintain a Firewall Configuration. A properly configured firewall could have prevented unauthorized access by blocking exploit attempts targeting CVE-2023-23397. CIS Control 4.7: Link
CS-RD	Citizen-centric Services - Prevent Reputational Damage	Reputational damage in citizen-centric services can erode public trust, especially if service disruptions or data breaches occur. Ensuring reliability, transparency, and quick incident response is key to maintaining citizen confidence.	M	H	A ransomware attack on a Dutch municipality (2024) leaked citizen data and disrupted services for a week, damaging public trust. Example: ENISA Public Administration TL 2024 (p. 35)	CVE-2023-27532: A vulnerability in Microsoft Exchange Server allowed ransomware deployment. CVE Details: NVD	CIS Control 10.1: Deploy and Maintain Anti-Malware Software. Anti-malware software could have detected and blocked ransomware payloads exploiting CVE-2023-27532. CIS Control 10.1: Link
CS-NS	Citizen-centric Services - Support National Security	Citizen-centric services may hold data critical to national security (e.g., immigration records, public health data). Protecting these services from espionage or sabotage ensures national stability.	M	VH	APT29 targeted Finnish immigration services (2023-2024), exfiltrating data on foreign nationals. Example: ENISA Threat Landscape 2025 (p. 37)	CVE-2023-4040: A vulnerability in Windows Message Queuing exploited for espionage. CVE Details: NVD	CIS Control 8.3: Configure Monitoring Systems to Record Packet Contents. Monitoring systems could have detected anomalous traffic patterns associated with CVE-2023-4040. CIS Control 8.3: Link

Combined Acronym	Full Title	Description	Current Probability	Current Impact	Example	Example CVE	Example Control
BS-OC	Business and Economic Services - Maintain Operational Continuity	Business and economic services (e.g., licensing, procurement) must remain operational to support economic activity. Disruptions can halt business operations, delay permits, or freeze transactions.	H	M	A DDoS attack on Belgium's business licensing portal (2024) halted operations for 12 hours, delaying permits for SMEs. Example: ENISA Threat Landscape 2025 (p. 19)	CVE-2023-38831: A vulnerability in F5 BIG-IP allowed DDoS amplification. CVE Details: NVD	CIS Control 13.2: Deploy a Denial-of-Service (DoS) Protection System. A DoS protection system could have mitigated DDoS amplification attacks exploiting CVE-2023-38831. CIS Control 13.2: Link
BS-DC	Business and Economic Services - Maintain Data Confidentiality/Integrity	Business services often manage proprietary or sensitive economic data (e.g., trade secrets, procurement bids). Ensuring data confidentiality and integrity prevents corporate espionage, fraud, or unfair competitive advantages.	H	H	The Tietoevry breach (2024) exposed procurement data for 120 Swedish agencies, disrupting business operations. Example: ENISA Public Administration TL 2024 (p. 22)	CVE-2023-34362: MOVEit Transfer SQL Injection Vulnerability, exploited for data exfiltration. CVE Details: NVD	CIS Control 3.10: Encrypt Sensitive Data in Transit. Encrypting data in transit could have prevented exploitation of CVE-2023-34362. CIS Control 3.10: Link
BS-RD	Business and Economic Services - Prevent Reputational Damage	Reputational damage in business services can deter investment or partnerships. Transparent, secure, and efficient services foster trust among businesses.	M	M	A data leak in a German procurement agency (2024) exposed bid details, leading to legal disputes and loss of business trust. Example: ENISA Public Administration TL 2024 (p. 24)	CVE-2023-22518: A vulnerability in Atlassian Confluence led to unauthorized data access. CVE Details: NVD	CIS Control 3.11: Encrypt Sensitive Data at Rest. Encrypting sensitive data at rest could have prevented unauthorized access to data via CVE-2023-22518. CIS Control 3.11: Link
BS-NS	Business and Economic Services - Support National Security	Business services tied to critical industries (e.g., defense contracting, energy) must be secured to prevent espionage or sabotage that could compromise national security or economic stability.	M	VH	China-nexus APT41 targeted EU defense contractors (2024), stealing proprietary data. Example: ENISA Threat Landscape 2025 (p. 39)	CVE-2023-20198: Cisco IOS XE Software Web UI Vulnerability, exploited for espionage. CVE Details: NVD	CIS Control 4.1: Establish and Maintain a Secure Configuration Process. Secure configurations could have prevented exploitation of CVE-2023-20198. CIS Control 4.1: Link
IE-OC	Infrastructure and Environment - Maintain Operational Continuity	Infrastructure services (e.g., transport, energy) are essential for societal functioning. Operational continuity ensures that critical systems like public transport, waste management, and energy grids remain functional.	H	M	A DDoS attack on Italy's transport management system (2024) disrupted train schedules for 6 hours. Example: ENISA Threat Landscape 2025 (p. 20)	CVE-2023-44487: HTTP/2 Rapid Reset Attack, exploited for DDoS. CVE Details: NVD	CIS Control 13.3: Configure a Reverse Proxy or Application Firewall. A reverse proxy could have mitigated HTTP/2 Rapid Reset attacks. CIS Control 13.3: Link

Combined Acronym	Full Title	Description	Current Probability	Current Impact	Example	Example CVE	Example Control
IE-DC	Infrastructure and Environment - Maintain Data Confidentiality/Integrity	Infrastructure systems often rely on sensitive operational data (e.g., grid configurations, transport schedules). Protecting this data ensures the integrity and security of critical infrastructure.	H	H	Lazarus Group compromised a European energy grid's SCADA system (2024), altering operational data. Example: ENISA Threat Landscape 2025 (p. 41)	CVE-2023-2286: Siemens SIMATIC S7-1500 CPU Denial-of-Service Vulnerability. CVE Details: NVD	CIS Control 6.1: Establish and Maintain an Inventory of Network Devices. Network device inventory could have helped isolate and patch systems vulnerable to CVE-2023-2286. CIS Control 6.1: Link
IE-RD	Infrastructure and Environment - Prevent Reputational Damage	Reputational damage in infrastructure services can undermine public confidence in essential systems. Reliable and secure infrastructure operations are vital to maintain trust.	M	H	A ransomware attack on a Spanish water management system (2024) disrupted services and leaked operational data, eroding public trust. Example: ENISA Threat Landscape 2025 (p. 28)	CVE-2023-27350: PaperCut MF/NG Improper Authentication Vulnerability, exploited for ransomware. CVE Details: NVD	CIS Control 10.2: Configure Automatic Execution Prevention. Automatic execution prevention could have blocked ransomware exploiting CVE-2023-27350. CIS Control 10.2: Link
IE-NS	Infrastructure and Environment - Support National Security	Infrastructure like energy grids or transport networks are national security targets. Securing these systems prevents adversaries from exploiting vulnerabilities to disrupt services or gain strategic leverage.	M	VH	Sandworm targeted Ukrainian energy infrastructure (2023-2024), causing blackouts. Example: ENISA Threat Landscape 2025 (p. 40)	CVE-2022-40684: Schneider Electric Modicon PLC Remote Code Execution Vulnerability. CVE Details: NVD	CIS Control 7.4: Use DNS Filtering Services. DNS filtering could have prevented command-and-control communication for exploits targeting CVE-2022-40684. CIS Control 7.4: Link
DA-OC	Digital and Administrative Services - Maintain Operational Continuity	Digital services (e.g., e-government portals) must remain available to support administrative functions. Downtime can disrupt citizen access to essential services.	H	M	A DDoS attack on the European Parliament's portal (2024) disrupted access for 8 hours during a key vote. Example: ENISA Threat Landscape 2025 (p. 18)	CVE-2023-44487: HTTP/2 Rapid Reset Attack, exploited for DDoS. CVE Details: NVD	CIS Control 13.1: Deploy a Web Application Firewall (WAF). A WAF could have filtered malicious HTTP/2 requests exploiting CVE-2023-44487. CIS Control 13.1: Link
DA-DC	Digital and Administrative Services - Maintain Data Confidentiality/Integrity	Digital services often handle sensitive citizen and government data. Ensuring confidentiality and integrity prevents data leaks that could lead to identity theft, fraud, or administrative disruptions.	H	H	The Estonian e-Governance breach (2024) exposed citizen IDs and tax records due to a misconfigured database. Example: ENISA Public Administration TL 2024 (p. 34)	CVE-2023-23752: Jira Data Center Authentication Bypass Vulnerability. CVE Details: NVD	CIS Control 4.8: Configure Firewall Rules to Block Unnecessary Services. Blocking unnecessary services could have prevented exploitation of CVE-2023-23752. CIS Control 4.8: Link

Combined Acronym	Full Title	Description	Current Probability	Current Impact	Example	Example CVE	Example Control
DA-RD	Digital and Administrative Services - Prevent Reputational Damage	Reputational damage in digital services can deter citizens from using online platforms. Secure, user-friendly, and reliable digital services are essential to maintain public trust and adoption.	H	H	A phishing campaign targeting French tax portal users (2024) led to credential theft and fraud, damaging trust. Example: ENISA Threat Landscape 2025 (p. 45)	CVE-2023-23397: Microsoft Outlook Elevation of Privilege Vulnerability, exploited for phishing. CVE Details: NVD	CIS Control 16.1: Implement Multi-Factor Authentication (MFA). MFA could have prevented credential theft via phishing exploiting CVE-2023-23397. CIS Control 16.1: Link
DA-NS	Digital and Administrative Services - Support National Security	Digital services may host classified or sensitive government data. Protecting these systems from cyber threats ensures national security and prevents adversaries from accessing strategic information.	H	VH	APT29 targeted EU digital diplomacy platforms (2024), exfiltrating sensitive communications. Example: ENISA Threat Landscape 2025 (p. 38)	CVE-2023-4040: Windows Message Queuing Vulnerability, exploited for espionage. CVE Details: NVD	CIS Control 17.1: Establish and Maintain a Security Awareness Program. Security awareness training could have helped staff recognize and report exploitation attempts of CVE-2023-4040. CIS Control 17.1: Link
CO-OC	Cross-cutting EU Compliance - Maintain Operational Continuity	Cross-cutting compliance services (e.g., fund management) must operate continuously to ensure EU policies and regulations are enforced without interruption, supporting cohesion across member states.	H	M	A DDoS attack on the EU Funds Portal (2024) disrupted grant applications for 10 hours. Example: ENISA Threat Landscape 2025 (p. 21)	CVE-2023-44487: HTTP/2 Rapid Reset Attack, exploited for DDoS. CVE Details: NVD	CIS Control 13.2: Deploy a Denial-of-Service (DoS) Protection System. A DoS protection system could have mitigated the HTTP/2 Rapid Reset attack exploiting CVE-2023-44487. CIS Control 13.2: Link
CO-DC	Cross-cutting EU Compliance - Maintain Data Confidentiality/Integrity	Compliance services handle sensitive data related to EU funds, regulations, and policies. Ensuring data confidentiality and integrity prevents misuse, fraud, or non-compliance with EU standards.	M	H	The European Anti-Fraud Office (OLAF) data leak (2024) exposed investigation details due to insufficient access controls. Example: ENISA Public Administration TL 2024 (p. 36)	CVE-2023-22518: Atlassian Confluence Unauthorized Access Vulnerability. CVE Details: NVD	CIS Control 3.11: Encrypt Sensitive Data at Rest. Encrypting sensitive data at rest could have prevented unauthorized access via CVE-2023-22518. CIS Control 3.11: Link
CO-RD	Cross-cutting EU Compliance - Prevent Reputational Damage	Reputational damage in compliance services can undermine the EU's credibility. Transparent and secure compliance mechanisms are essential to maintain trust among member states and citizens.	M	H	A misconfiguration in the EU's Schengen Information System (2024) exposed traveler data, leading to public outcry. Example: ENISA Public Administration TL 2024 (p. 37)	CVE-2023-23866: Oracle Access Manager Authentication Bypass Vulnerability. CVE Details: NVD	CIS Control 4.7: Deploy and Maintain a Firewall Configuration. A properly configured firewall could have blocked unauthorized access attempts exploiting CVE-2023-23866. CIS Control 4.7: Link

Combined Acronym	Full Title	Description	Current Probability	Current Impact	Example	Example CVE	Example Control
CO-NS	Cross-cutting EU Compliance - Support National Security	Compliance with EU-wide security standards (e.g., NIS2, GDPR) is critical to national security. Ensuring adherence to these frameworks prevents vulnerabilities that adversaries could exploit.	M	VH	Non-compliance with NIS2 directives (2024) in a member state left critical infrastructure vulnerable to attacks. Example: ENISA Threat Landscape 2025 (p. 42)	CVE-2023-20864: VMware Aria Operations for Logs RCE Vulnerability, exploited for non-compliance. CVE Details: NVD	CIS Control 3.12: Implement and Maintain a Patch Management Process. Regular patching could have prevented exploitation of CVE-2023-20864. CIS Control 3.12: Link

Appendix A: How to use this report

The principal risks refer to the most significant or critical risks that a public administration faces, which could have a major impact on its objectives, operations, reputation, or survival. For this report, the principal risks are based on the priorities and processes as defined by ENISA.

The aim of every EU public administration could be to (a) align their risks with the principal risks, (b) review the regular principal risk reports to align their risk management with EU level directives, acts, policies and procedures, and (c) submit their top level risks to this report process to enhance the principal risk assessment.

Key characteristics of principal risks are:

1. Principal risks have the potential to cause severe impact.
2. They are likely to occur based on historical data, threat intelligence, or emerging trends.
3. Principal risks are aligned with the core objectives or mission of public administrations.
4. Principal risks demand immediate and sustained attention.

This is report aims to support national, regional, and local public administrations in aligning their risks to the principal risks. Aligning national, regional, and local risk management efforts to the principal risks for Public Administrations offers significant strategic, operational, and financial benefits.

1. Strategic Benefits

A. Unified Risk Prioritization

- Focus on What Matters Most: Principal risks (e.g., state-nexus espionage, ransomware, DDoS attacks) are identified as the highest-impact, highest-probability threats to Public Administrations. Aligning all levels (national, regional, local) ensures that resources, policies, and efforts are directed toward mitigating these critical risks first, rather than fragmented or lower-priority concerns.

- Avoids Duplication: Prevents redundant risk management activities across different levels of government. For example, if DDoS protection (CIS 13.2) is a principal risk mitigation strategy, national, regional, and local entities can coordinate their defenses rather than implementing isolated solutions.

B. Improved Decision-Making

- Consistent Risk Appetite: Alignment ensures that risk tolerance (e.g., for data breaches or operational disruptions) is standardized across all levels. This prevents conflicts where one level accepts a risk that another cannot tolerate (e.g., a local government accepting a moderate risk of data exposure while the national level classifies it as unacceptable).

- Informed Resource Allocation: National budgets can prioritize funding for principal risks (e.g., NIS2 compliance, zero-trust architecture) that also address regional and local concerns. For example, investing in national-level DDoS protection benefits all lower levels.

C. Enhanced National Security

- Holistic Threat Response: Principal risks like state-nexus espionage (APT29, Sandworm) or critical infrastructure sabotage often transcend local or regional boundaries. Alignment ensures a coordinated response (e.g., sharing threat intelligence, joint incident response plans) rather than siloed efforts.

- Compliance with EU/National Directives: Many principal risks (e.g., GDPR non-compliance, NIS2 vulnerabilities) are tied to legal or regulatory obligations. Alignment ensures that local and regional entities meet national and EU-wide standards, avoiding fines or reputational damage.

2. Operational Benefits

A. Efficient Resource Utilization

- Shared Tools and Frameworks: National-level investments in cybersecurity frameworks (e.g., CIS Controls, ISO 27001) or threat intelligence platforms can be leveraged by regional and local entities, reducing costs and improving effectiveness. For example:

  - A national WAF (Web Application Firewall) can protect regional and local e-government portals from DDoS attacks.
  - Centralized patch management (CIS 3.12) can ensure all levels are protected against exploited CVEs (e.g., CVE-2023-44487).

- Economies of Scale: Pooling resources for principal risk mitigation (e.g., cloud-based DDoS protection, encryption tools) lowers costs for smaller entities (e.g., local governments) that might not afford these solutions independently.

B. Standardized Processes

- Common Risk Assessment Methodologies: Using the same probability-impact matrices and threat intelligence sources (e.g., ENISA, EUVD) across all levels ensures consistency in risk identification and prioritization. For example:
  - A DDoS attack assessed as High Probability/Moderate Impact (H/M) at the national level should be treated similarly at regional and local levels.
- Uniform Incident Response: Aligned playbooks for principal risks (e.g., ransomware, data breaches) ensure that all levels respond effectively to incidents. For example:
  - A ransomware playbook developed nationally can be adapted for regional or local municipalities.

C. Improved Collaboration

- Threat Intelligence Sharing: National agencies (e.g., ENISA, CSIRTs) can disseminate real-time threat data (e.g., new APT campaigns, exploited CVEs) to regional and local entities, enabling proactive mitigation. For example:
  - If APT29 targets immigration data (a principal risk for CS-NS), local immigration offices can heighten monitoring for related CVEs (e.g., CVE-2023-4040).
- Joint Exercises: Aligned principal risks enable cross-level cybersecurity drills (e.g., simulating a supply chain attack on a national vendor that affects local services).

3. Financial Benefits

A. Cost Savings

- Reduced Redundancy: Avoids duplicate investments in tools or processes. For example:
  - Instead of each region purchasing its own DDoS protection system, a national system can cover all levels.
- Bulk Purchasing Power: National or regional procurement of cybersecurity solutions (e.g., firewalls, encryption tools) can lower costs for local entities through volume discounts.

B. Risk Transfer and Insurance

- Pooled Risk Management: National or regional cyber insurance policies can cover local entities, reducing individual premiums while ensuring comprehensive protection against principal risks (e.g., data breaches, ransomware).
- Shared Liability: Aligning to principal risks ensures that liability for incidents (e.g., GDPR fines for data breaches) is distributed appropriately across levels, rather than falling disproportionately on local entities.

4. Reputational Benefits

A. Public Trust and Transparency

- Consistent Messaging: Aligned risk management ensures that communication to citizens about threats (e.g., phishing campaigns, service disruptions) is cohesive and trustworthy. For example:
  - If a national data breach occurs, local entities can reference the same mitigation steps (e.g., MFA, encryption) to reassure citizens.

- Accountability: Clear alignment to principal risks demonstrates due diligence to stakeholders (e.g., EU auditors, citizens), reducing reputational damage from incidents.

B. Cross-Border Credibility

- EU-Wide Compliance: Many principal risks (e.g., NIS2, GDPR) are tied to EU directives. Alignment ensures that all levels meet these standards, enhancing the EU's credibility and avoiding sanctions.
- International Cooperation: Aligned risk management facilitates collaboration with international partners (e.g., NATO, Interpol) on cross-border threats like state-nexus espionage.

5. Challenges of Misalignment

If risks are not aligned across levels, the following issues can arise:

1. Fragmented Defenses: Local entities may underestimate principal risks (e.g., ignoring state-nexus espionage) while over-focusing on low-impact threats.
2. Resource Waste: Redundant or conflicting cybersecurity tools (e.g., multiple DDoS protection systems) drain budgets.
3. Compliance Gaps: Local entities may fail to meet national/EU standards (e.g., NIS2, GDPR), leading to fines or legal consequences.
4. Slow Incident Response: Lack of shared playbooks or threat intelligence delays responses to principal risks (e.g., ransomware, data breaches).
5. Reputational Harm: Inconsistent messaging or poorly managed incidents erode public trust in all levels of government.

Appendix B: Barista Description

Title

Generative AI Agent for Simulating Chief Information Security Officer (CISO) Functions for European Union Public Administrations

Creator: Oliver Schwabe

Barista AI Agent Character

Barista is a proprietary generative AI agent designed to simulate the role of a Chief Information Security Officer (CISO) for public administrations across the European Union (EU). Barista operates under a cyber risk management philosophy aligned with EU regulations, maintaining a principal risk register for EU public administrations. It encourages alignment of national and local risk registers with this principal structure. Barista's tone is objective and direct, focusing on actionable insights and solutions within a principal risk approach, while leveraging CIS Controls as a universal framework for cybersecurity best practices.

BACKGROUND

Field of Activity

Barista pertains to the field of artificial intelligence (AI)-driven cybersecurity, specifically for public sector risk management and regulatory compliance in the EU. It addresses the need for a standardized, AI-powered CISO simulation to assist public administrations in aligning with EU cybersecurity directives, policies, and procedures.

Prior Art

Traditional cybersecurity frameworks for public administrations rely on manual risk assessments, fragmented compliance tools, and human-led CISO roles. These approaches often lack:

- Scalability across diverse national and local administrations.
- Real-time alignment with evolving EU regulations (e.g., NIS2, GDPR, DORA).
- Automated risk register synchronization between principal and subsidiary entities.
- Consistent interpretation of global cybersecurity controls (e.g., CIS Controls).

Existing AI solutions (e.g., chatbots, rule-based systems) fail to provide a holistic, regulation-aligned CISO simulation tailored for the EU public sector.

SUMMARY OF BARISTA

Barista is a generative AI agent that:

1. Simulates a CISO for EU public administrations, providing risk management, compliance guidance, and incident response support.
2. Operates a principal risk register for the EU, encouraging alignment of national/local registers with this structure.
3. Aligns with EU directives (e.g., NIS2, GDPR, Cybersecurity Act) and global frameworks (e.g., CIS Controls).
4. Delivers actionable insights in an objective, direct tone, prioritizing principal risk approaches.
5. Automates compliance checks, threat hunting, and remediation guidance using natural language processing (NLP) and machine learning (ML).

Key Features

- Regulation-Aware Decision Engine: Interprets and applies EU cybersecurity directives (e.g., NIS2, DORA) in real time.

- CIS Controls Integration: Uses CIS Controls as a universal language for cybersecurity best practices.
- Multi-Jurisdictional Compliance: Adapts guidance for cross-border public administrations (e.g., shared infrastructure, data flows).

DETAILED DESCRIPTION

System Architecture

Barista comprises the following core components:

1. Regulatory Alignment Module
    - Input: EU directives (e.g., NIS2, GDPR), national laws, and local policies.
    - Output: Compliance gap analysis and remediation roadmaps.
    - Mechanism: Uses NLP to parse legal texts and knowledge graphs to map dependencies between regulations.
2. Principal Risk Register
    - Centralized Database: Stores EU-wide cyber risks (e.g., critical infrastructure threats, data breach patterns).
    - Risk Scoring: Assigns severity scores based on likelihood, impact, and regulatory penalties.
3. Generative AI Core
    - Model: Fine-tuned large language model (LLM) trained on:
        - EU cybersecurity documents (e.g., ENISA reports, NIS2 guidance).
        - CIS Controls v8 and MITRE ATT&CK frameworks.
        - Historical incident response data from public administrations.
    - Capabilities:
        - Natural Language Queries: Answers questions like *"How does NIS2 affect our municipal IT systems?"*

Method of Operation

1. Ingestion Phase
    - Barista scrapes/ingests the latest EU directives, threat reports, and CIS Controls updates.
    - Normalizes data into a unified risk ontology.
2. Query Phase
    - Public administration users submit queries (e.g., *"What are the NIS2 requirements for our IT?"*).
    - Barista generates responses with:
        - Regulatory citations (e.g., NIS2 Article 21).
        - Actionable steps (e.g., "Implement MFA for all privileged accounts").
        - Risk prioritization (e.g., "Critical: Patch CVE-2023-1234 within 72 hours").

CLAIMS

1. A generative AI system for simulating a CISO role in EU public administrations, comprising:
    - A regulatory alignment module configured to interpret and apply EU cybersecurity directives.
    - A natural language interface for querying compliance and risk management guidance.

2. The system of Claim 1, wherein the regulatory alignment module uses NLP to parse legal texts and knowledge graphs to map regulatory dependencies.
3. The system of Claim 1, wherein the principal risk register assigns risk scores based on EU-specific threat intelligence.
4. The system of Claim 1, wherein the generative AI core is fine-tuned on CIS Controls, MITRE ATT&CK, and ENISA guidelines.
5. A method for aligning cybersecurity risk registers across EU public administrations, comprising:
    - Ingesting EU directives and CIS Controls.
    - Comparing national/local registers against a principal EU register.
    - Generating remediation recommendations for compliance gaps.
6. The method of Claim 6, further comprising automatically updating national/local registers via secure APIs.
7. A computer-readable medium storing instructions that, when executed, cause a system to perform the method of Claim 6.

INDUSTRIAL APPLICABILITY

Barista is applicable to:

- National governments (e.g., Germany's BSI, France's ANSSI).
- Municipal administrations (e.g., city councils, regional IT departments).
- EU agencies (e.g., European Commission, Europol).
- Critical infrastructure operators (e.g., healthcare, energy, transport).

Intellectual Property Protection

Copyright

Element	Description
Sigma Rule Templates	Custom detection rules for public sector threats.

Trade Secrets

Element	Description
Barista Agent Design	Unique design of character and behaviour optimised for role.
Model Weights	Fine-tuned parameters for the Barista threat detection model.
Proprietary Datasets	Classified threat intelligence data from EU public sector networks.

DATA SOURCES

1. MITRE ATT&CK
2. NIS2 Directive (Network and Information Security Directive)
3. GDPR (General Data Protection Regulation)
4. Cybersecurity Act
5. Critical Entities Resilience Directive (CER)
6. EU Cybersecurity Strategy
7. ENISA (European Union Agency for Cybersecurity) Guidelines

8. ECCC (European Cybercrime Centre) at Europol
9. EU Digital Operational Resilience Act (DORA)
10. EU Cloud Rulebook
11. EU Toolbox for 5G Security
12. CIS Controls v8