Cybersecurity as the New Frontier of Project Management in Public Administration[1]

Luca Paolo Giuseppe Prinzio

Abstract

Cybersecurity is today a strategic priority for Public Administration. This article shows how the Project Manager can transform security from a technical obligation into a lever for public value, integrating regulations, methodologies, and organisational culture. With agile approaches, AI, and structured governance, project management becomes a tool for resilience, trust, and sustainable innovation.

Introduction

Information security in Public Administration is not a separate technical compartment, but the backbone of the State's ability to deliver services, protect rights, and ensure institutional continuity. The cloud, in its various declinations—proprietary or public poles—has made the application lifecycle more efficient but has structurally expanded the attack surface. Today, registries, healthcare systems, taxes, territorial information assets, digital education, and telematic justice live on distributed infrastructures, with complex dependencies between data centers, networks, platforms, and suppliers. In this scenario, the Project Manager is not the custodian of the Gantt chart; they are the director who organises technology, processes, and people to transform cybersecurity from a perceived cost into a generator of public value, translating compliance into governance and adherence into measurable resilience. The starting point is not the list of controls, but the definition of value: which services must remain operational under all conditions, with what service levels, at what cost, and with what recovery priorities. It is here that project management shows its enabling nature: integrating different viewpoints, aligning choices with strategy, and making security sustainable throughout the entire service lifecycle.

[1] How to cite this work: Prinzio, L. P. G. (2026). Cybersecurity as the New Frontier of Project Management in Public Administration, *PM World Journal*, Vol. XV, Issue IV, April.

The Changing Context

The context has irreversibly changed. The armed conflicts of recent years have opened a second stable front, the digital one, in which state and non-state groups use malware, targeted phishing campaigns, DDoS attacks, sabotage against civilian infrastructures, and influence operations. A "hybrid war" that knows no borders and makes even administrations not directly involved possible collateral targets, vectors of disinformation, or pawns of geopolitical pressure. The European Public Administration cannot read these phenomena as remote risks: the legislator has reacted with the NIS2 Directive, which imposes risk management measures, notification obligations, and supervision rules for a wide range of essential and important entities, including administrations and operators of fundamental services. The effect for the Project Manager is concrete: hardening, migration, or rationalisation projects must include from the outset a design of organisational and technical controls, reporting flows, and effectiveness metrics proportionate to the service risk, as well as a coordination mechanism with national authorities and CSIRTs. (EUR-Lex)

This regulatory framework builds on already known obligations. GDPR, in Article 32, requires technical and organisational measures adequate to the risk, including encryption and pseudonymisation, and processes to regularly assess and test the effectiveness of measures. It is a mandate for risk engineering, not a list of products; it requires proportionality, traceability, and continuous verification. A Project Manager planning the hardening of a service with personal data must treat security as a quality and cost requirement: encryption, access segregation, key rotation, network segmentation, and log controls are not optional but design criteria, supplier selection, and testing. The frequent mistake is considering security "added later", with residual budgets and compressed timelines; the result is fragile, ungovernable solutions, incapable of passing meaningful audits and lasting over time. (GDPR)

Best Practices and Standards

The best practice framework does not end with regulations. ISO/IEC 27001 defines the requirements for an Information Security Management System (ISMS) based on a process approach and continuous improvement; ISO 22301 structures business continuity and recovery after disruptive events. These standards translate the essential intuition for Public Administration: security is not a project that "ends", it is a management system that lives. Inserting controls into an ISMS and anchoring RTOs/RPOs to a BCMS reduces dependence on key individuals, makes service promises measurable, and allows conscious negotiation of priorities and trade-offs. A Project Manager must know how to use standards as an organisational contract: requirements, roles, audits, indicators, improvement plans, and

periodic exercises. Without this discipline, every technical measure remains tactical and degrades over time. (ISO)

The theme of cyber war makes the structural weak points of the public sector more evident: layering of legacy applications, slow procurement cycles, scarce skills and high turnover, heterogeneous integrations, spending constraints. In Italy, the National Cybersecurity Strategy and the National Cyber Perimeter were created precisely to fill these fragilities, coordinate institutional actors, give coherence to prevention, response, and recovery, and promote national capabilities and European relations. For the Project Manager, this means moving in an ecosystem with clear rules and interlocutors, with alert channels, defined responsibilities, minimum requirements, and notification processes. The project is no longer an isolated initiative; it is a piece of a national posture: it must respect perimeters, prepare asset inventories, classify information, and ensure collaboration with CSIRTs and supervisory bodies. (acn.gov.it)

The Project Manager's First Lever: Value-Oriented Planning

The Project Manager's first lever is value-oriented planning. In the initial phase, a security business case must be built that speaks the language of executives: risk avoided, reduced service impacts, lower operational losses, lower legal and reputational costs, greater perceived reliability by citizens. Cost analysis must include often ignored items: encryption and KMS licences, monitoring platforms and SIEM, storage for logs and legal retention, segmentation CAPEX, key and certificate management OPEX, audit and penetration test costs, continuous training, DR exercises, cyber insurance. Budget construction must be accompanied by a skills plan, internal and external: which profiles are needed, who covers them, how team continuity is guaranteed, which activities are outsourced and with what SLAs and contractual clauses on incident response, evidence, and chains of custody.

The Second Lever: Stakeholder Management

The second lever is stakeholder management. Public Administration lives with a plurality of interests: ICT directorates, responsible for proceedings, legal offices, data protection officers, control bodies, reference departments or ministries, suppliers, and sometimes academic partners. The Project Manager must map influence and interest, define expectations, and build a common narrative connecting technical risks to service and policy impacts. The PRINCE2 practice of "continued justification" and the PMBOK discipline of performance domains allow maintaining course: deciding by phases, managing by exception, measuring adherence to expected outcomes, recalibrating priorities and backlogs in light of evidence. In security, management by exception works if tolerance

thresholds are clear: maximum response times, patching windows, vulnerability backlogs with severity levels, KPIs and KRIs on detection and containment. (axelos.com)

Hybrid Method

The method must be hybrid. The predictive part serves for assessment, procurement, compliance, contractual integration, and approvals; the iterative part serves for incremental releases of controls, logging tuning, progressive hardening, policy as code, resilience testing, and continuous improvement. "Progress iteratively with feedback", a cardinal principle of ITIL 4, is a perfect synthesis of how to design security in complex environments: small steps, objective evidence, rapid corrections, transparent visibility towards stakeholders, value perceivable from the first sprints. In parallel, "Focus on value" and "Collaborate and promote visibility" recall the need to show measurable impacts on services and to work with multiple teams without creating silos. (axelos.com)

Operational Techniques as Security Governance Tools

The Project Manager's operational techniques must become security governance tools, not just delivery tools. The WBS does not list generic activities, but work packages reflecting controls and capabilities: data classification and BIA, network segmentation, identity and privilege management, at-rest and in-transit encryption, KMS and key rotation, logging and event correlation, vulnerability and patch management, penetration testing and code review, DR plan and recovery tests, training and awareness, incident response runbooks, audit trail, improvement cycle. The RACI matrix must resolve ambiguities between who decides and who operates: Risk Responsible, Data Protection Officer, service owner, security architect, dev lead, operations, internal audit. Risk management is alive: risk register linked to backlog, priority based on service impact and probability, documented response (mitigate, transfer, accept, avoid), remediation speed, and explicit security debt.

Business Continuity

The dimension of business continuity is part of the project content, not an addendum. Every critical service must have an updated BIA, negotiated and subscribed RTOs and RPOs, tested recovery environments, periodic exercises with realistic scenarios, and internal and external communication playbooks. ISO 22301 provides structure and shared language to integrate these elements into the project and then into operations. The difference between a managed incident and a systemic crisis is rarely technological: it is in reaction time, role clarity, and team training. An effective Project Manager plans exercises as part of the

schedule, measures them with recovery time KPIs and data quality, uses them to feed the lesson-learned cycle, and updates plans and contracts. (ISO)

The Adoption of AI

The adoption of AI changes the way security is designed and managed. On the SecOps front, machine learning models detect anomalies in network flows, correlate events in real time, learn behaviour patterns, and signal deviations with confidence levels, reducing detection times and false positives. On the project management front, AI feeds schedule slippage predictions, suggests resource reallocations, estimates the impact of risks and dependencies, proposes mitigation scenarios, and calculates alternative economic consequences. Adoption is not neutral: data governance, model explainability, algorithmic risk management, threshold quality control, and human supervision are needed to avoid dangerous automatisms. The Project Manager must define validation criteria, data retention and access policies, and introduce accuracy and drift metrics, with tuning cycles fully entering the plan.

Cultural Posture

Even cultural posture is a project. Most serious incidents stem from incorrect behaviours or un-respected processes: weak or shared credentials, disabled MFA, opened malicious attachments, shadow IT, "temporary" environments never decommissioned, accumulated permissions. Training cannot be a one-off course. It must be scheduled by role, measured with practical exercises and simulated phishing campaigns, and linked to residual risk and internal compliance metrics. The Project Manager includes these streams in the plan, funds them, measures their outcomes, and reports on them in the project committee. Security culture develops when users see the relationship between daily behaviour and service quality, when executives link investments to event reduction, when auditors detect growing maturity. Indicators are not esoteric: rate of critical vulnerabilities open beyond SLA, remediation time, MFA coverage, percentage of source logs indexed, automatically vs manually detected events, DR exercise results.

National Context

In the national public domain, signals are clear. Periodic reports from CERT-AgID show the variety and volume of malicious campaigns targeting the Italian perimeter, with growing use of trusted channels like certified email (PEC), tax themes, or cloud services to deliver phishing and malware. This says two operational things: defence is also a matter of basic

digital hygiene, and communication must be capillary, concrete, and timely. Planning an internal alert channel in the project, a kit of pre-approved messages, and a direct line with the national CERT reduces friction in the first hours of an incident and increases the chance of containing damage. Institutional cooperation is not a matter of image; it is a resilience functionality. (CERT-AGID)

Methodological Frameworks

From a methodological point of view, the modern PM has a rich set available. PMBOK 7 shifts attention from prescriptive processes to performance domains: stakeholder, team, development and lifecycle, planning, delivery, measurement, uncertainty. This language adapts well to security, where uncertainty is structural and results are measured on service outcomes. PRINCE2, with its principles of management by phases, continued justification, defined roles, and management by exception, offers a governance structure that integrates with PMI domains. ITIL 4 adds the logic of value, visibility, and continuous improvement, useful for connecting the project with operations and the service portfolio. The Project Manager's skill lies in tailoring: choosing sensible combinations, adopting light but effective artefacts, avoiding redundancies, ensuring every document lives and serves decisions. (pmi.org)

Daily Practice Suggestions

Daily practice suggests some robust choices. Firstly, "security by design and by default": security requirements inserted in user stories, definitions of "done" including tests and log coverage, policy as code in tracked repositories, CI/CD pipelines with scanning and quality gates, centralised secret management, documented and versioned configuration invariants. Then, "sensible segregation": separate environments, accounts, networks, and roles not for fetishism but to reduce the impact radius, simplify audits, and accelerate recoveries. Next, "observability before automation": without complete logs, consistent timestamps, correlation, and meaningful alerts, every response automation risks amplifying errors. Finally, "contracts as security tools": realistic SLAs and SLOs, targeted but applicable penalties, transparency requirements on incidents, supply-chain security obligations and software bill of materials, audit rights, data and backup rules, data residency and end-to-end encryption constraints.

Typical Challenges in Cloud Security Projects

A security project in proprietary public cloud or public poles must face typical challenges. The first is data classification and definition of minimum requirements per class, to combine protections and costs rationally. The second is key management: where they reside, who governs them, with what rotation and recovery procedures; the KMS is not an accessory, it is critical infrastructure. The third is log quality: sources, formats, timings, retention consistent with regulations and investigations, search and alerting capability, budget for indexing and storage. The fourth is vulnerability management: reliable inventories, negotiated patching windows, emergency mechanisms for critical vulnerabilities, separation between test and production, rollback criteria. The fifth is mandatory training and live testing: awareness and crisis plans seriously exercised, with measurements and corrections. A Project Manager must make visible the chain from requirement to expenditure to effect on residual risk, because only what is visible enters decisions.

European Digital Sovereignty

There is also the dimension of European digital sovereignty. ENISA highlights the need to strengthen common capabilities, build European vulnerability databases, promote homogeneous practices across Member States, and support the resilience of public bodies, still often exposed due to budget constraints and legacy. This context links local Public Administration objectives to a broader design: standardisation, information sharing, alignment with technical guidelines for NIS2 implementation, with particular attention to supply chain risk management and cross-border cooperation. For the Project Manager, this means the project does not have to reinvent the wheel: it can draw on technical guides, evaluation frameworks, and shared good practices to accelerate, reduce errors, and improve the quality of evidence to present to supervisors. (Financial Times)

Operational Techniques

On the operational level, some techniques deserve a permanent place. The priority matrix by risk and value helps order backlogs and investments: not all controls have the same cost/benefit ratio. The technique of "minimum resilience paths" identifies indispensable elements to guarantee minimally acceptable continuity and directs budget and efforts first to segmentation, identity, immutable backups, and recovery. "Guardrail policies" fix a few inviolable, easy-to-verify constraints: mandatory MFA for administration, encryption by default for archiving, prohibition of direct management exposure, standardised system logging with minimum retention, four-eyes approval obligation for modifying security

criteria. "Continuous verification" brings weekly or monthly automatic checks on configuration drift and risk postures, with trends feeding decision-making committees.

Measuring to Govern

The Project Manager measures to govern. Useful metrics are not infinite and must not be decorative. A few robust, stable measures linked to objectives suffice: average detection and containment time, percentage of inventoried assets compared to estimated total, coverage of critical patches within SLA, success rate of recovery exercises, outcome of simulated phishing campaigns, percentage of systems with complete logging and SIEM integration, estimated security debt and reduction trend. These metrics, presented regularly, enable decision-makers to allocate resources wisely, appreciate progress, and correct drifts. The Project Manager must transform numbers into choices: if containment time does not improve, playbooks, roles, escalation, or tools need revision; if MFA coverage stagnates, constraints or incentives need revisiting; if DR tests fail, the plan is paper and needs re-engineering.

Common Mistake: Security as Discrete Purchases

A common mistake in administrations is approaching security as a set of discrete purchases. One buys an endpoint solution, a firewall, a SIEM, a KMS, but without a coherent design and without exercise capacity. The result is a constellation of underutilised tools, incomplete integrations, ignored alarms, generated but unread reports. The Project Manager must oppose this drift with a simple principle: every component enters only if placed in a process architecture, with roles, metrics, and responsibilities, and if a realistic adoption plan exists. Even the choice not to do must be made explicit: not everything is economically sustainable, not everything is a priority; value lies in selection, not accumulation.

Agile Methodologies

Recourse to agile methodologies is not fashion, it is a response to a world that changes faster than specifications. Security is not planned once and for all; it is released in iterations, tested, measured, and corrected. Public Administration can and must work in a hybrid way: predictive on legal and contractual parts, iterative on release and tuning of controls, with sprint review cadence involving non-technical decision-makers. In this setup, the Project Manager becomes a facilitator of organisational learning, avoids lock-in on wrong choices, reduces the risk of long projects arriving late on already mutated threats. ITIL 4 principles on

collaboration and visibility are the cultural guide to avoid micromanagement and bring problems to light where they can be solved. (axelos.com)

European Trends

Looking at Europe, trends show a clear direction: strengthening of ENISA, European vulnerability databases, standardisation of practices, and push for NIS2 implementation in still fragile sectors like public administration, healthcare, and water. For the Project Manager, this means opportunities: templates, technical checklists, governance models, and self-assessment tools can be reused. It also means responsibility: projects must anticipate regulatory evolution, improve the digital supply chain, and ask partners for transparency and security levels consistent with European requirements. Supply-chain security is not an attachment; it is often the breaking point, and must be treated with targeted contracts, conformity evidence, periodic attestations, and agreed reaction capabilities. (Financial Times)

Conclusion: From Vulnerability to Resilience

Drawing conclusions, the difference between a vulnerable and a resilient organisation lies not in the quantity of technology but in the quality of management. The Public Administration Project Manager is the architect of this quality. They establish priorities, build teams, align stakeholders, implement standards and regulations, integrate AI in a governed way, create culture and transparency, make risk understandable and negotiable. They are the figure who transforms obligation into choice, fear into method, budget into capability. Security ceases to be a superstructure and becomes an intrinsic characteristic of public service, designed, measured, and improved over time. In an era of hybrid war and complex dependencies, this is perhaps the most concrete form of digital sovereignty at the administrative level: the ability to continue serving citizens reliably and verifiably, despite attacks, failures, and uncertainties. It is a demanding objective but within reach of those who govern projects with discipline, competence, and vision. (acn.gov.it)

Note on AI Usage

During the preparation of this article, artificial intelligence tools were used solely to assist in translation from Italian to English and to improve the linguistic clarity of the text. All content, analyses, arguments, and conclusions are entirely the work of the author, who maintains full responsibility for the originality, accuracy, and validity of the presented work. No part of the substantive content was generated by AI.

Bibliography

1. Regulatory Sources

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)*. Official Journal of the European Union L119. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union L333/80. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

International Organization for Standardization (ISO). (2019). *ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements*. Geneva, CH: ISO. https://www.iso.org/standard/75106.html

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva, CH: ISO. https://www.iso.org/standard/82875.html

Italian Republic. (2005). *Legislative Decree 7 March 2005, n. 82 – Digital Administration Code (CAD)*. Official Gazette of the Italian Republic. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005;82

Italian Republic. (2019). *Law 18 November 2019, n. 133 – Establishment of the National Cyber Security Perimeter (PSNC)*. Official Gazette of the Italian Republic. https://www.gazzettaufficiale.it/eli/id/2019/12/09/19G00157/sg

---

2. Project Management and IT Governance Frameworks and Standards

AXELOS. (2009). *Managing Successful Projects with PRINCE2 (2009 ed.)*. London, UK: The Stationery Office. https://www.axelos.com/best-practice-solutions/prince2

AXELOS. (2019). *ITIL® 4 Foundation: ITIL 4 Edition*. London, UK: The Stationery Office. https://www.axelos.com/certifications/itil-4-foundation

International Project Management Association (IPMA). (2006). *ICB Version 3.0 – IPMA Competence Baseline for Project, Programme & Portfolio Management*. Amsterdam, NL: IPMA. https://www.ipma.world/

Project Management Institute (PMI). (2021). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition*. Newtown Square, PA: Project Management Institute. https://www.pmi.org/pmbok-guide-standards

U.S. Department of Defense. (2021). *Enterprise DevSecOps Reference Design*. Washington, DC: DoD Chief Information Office. https://dodcio.defense.gov/Library/Reference-Design/

3. Institutional Sources, National and European Agencies

Agency for National Cybersecurity (ACN). (2022). *National Cybersecurity Strategy 2022–2026*. Rome, IT: Presidency of the Council of Ministers. https://www.acn.gov.it/strategia-nazionale-cybersicurezza

Agency for Digital Italy (AgID). (2021). *Guidelines for ICT Security of Public Administrations*. Rome, IT: AgID. https://www.agid.gov.it/it/sicurezza

CERT-AgID / CSIRT Italia. (2024). *National Cybersecurity Report 2024*. Rome, IT: Agency for National Cybersecurity. https://www.csirt.gov.it/report

CSIRT Italia. (2023). *Guidelines on Cyber Incident Management in Public Administration*. Rome, IT: Agency for National Cybersecurity. https://www.csirt.gov.it/documentazione

ENISA – European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023*. Athens, GR: ENISA Publications Office. https://www.enisa.europa.eu/topics/threats-and-trends

ENISA – European Union Agency for Cybersecurity. (2024). *Guidelines on Security Measures under the NIS2 Directive*. Athens, GR: ENISA Publications Office. https://www.enisa.europa.eu/publications

Garante per la Protezione dei Dati Personali. (2022). *Guidelines on Data Breach and Data Security*. Rome, IT. https://www.garanteprivacy.it/temi/sicurezza

European Commission. (2024). *Cybersecurity and Resilience of Critical Entities – Digital Europe Programme*. Brussels, BE: European Commission. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity

4. Reports, Studies, and Reference Cases

Accenture. (2024). *The Cyber-Resilient Organization: Building Trust in a Hybrid World*. Dublin, IE: Accenture Security. https://www.accenture.com/it-it/insights/security

Clusit – Italian Association for Information Security. (2024). *Clusit Report 2024 on ICT Security in Italy*. Milan, IT. https://www.clusit.it/rapportoclusit/

Gartner. (2023). *Emerging Technologies and Trends Impact Radar: Security*. Stamford, CT: Gartner Research. https://www.gartner.com/en/information-technology

IBM Security & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. Armonk, NY: IBM Security. https://www.ibm.com/reports/data-breach

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Redmond, WA: Microsoft Corporation. https://www.microsoft.com/en-us/security/business/security-intelligence-report

NIST – National Institute of Standards and Technology. (2024). *Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF 2.0)*. Gaithersburg, MD: U.S. Department of Commerce. https://www.nist.gov/cyberframework

CISA – Cybersecurity & Infrastructure Security Agency. (2023). *Shields Up: Guidance for Critical Infrastructure and Government Entities*. Washington, DC: U.S. Department of Homeland Security. https://www.cisa.gov/shields-up

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. Geneva, CH: World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

Google Cloud. (2024). *State of DevSecOps 2024 – Google Cloud Security Whitepaper*. Mountain View, CA: Google Cloud. https://cloud.google.com/security

5. Methodological and Academic References

AXELOS. (2020). *ITIL® 4 Managing Professional – High Velocity IT*. London, UK: The Stationery Office.

ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. Rolling Meadows, IL: ISACA.

IPMA. (2016). *Project Excellence Baseline (PEB)*. Amsterdam, NL: International Project Management Association.

Project Management Institute. (2019). *The Standard for Risk Management in Portfolios, Programs, and Projects (2nd ed.)*. Newtown Square, PA: Project Management Institute.

ENISA. (2023). *European Cybersecurity Skills Framework (ECSF)*. Athens, GR: ENISA Publications Office. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework

ACN & Politecnico di Milano. (2024). *Report on Digital Security of the Italian Public Administration 2024*. Rome, IT: Agency for National Cybersecurity.

Forum PA & AgID. (2023). *Cybersecurity in Public Administration: Culture, Skills, Organisational Models*. Rome, IT: FPA Digital 360.

6. Cited or Derived Applied Cases from Public Best Practices

CSI Piemonte & City of Turin. (2023). *Public Administration Cloud Migration Project with Logical Segmentation, KMS Encryption, and Centralised Logging*. Turin, IT: Internal Documentation.

Lepida S.c.p.A. – Emilia-Romagna Region. (2023). *Adoption of DevSecOps Model and Security by Design in Regional Cloud Services*. Bologna, IT: Emilia-Romagna Region.

Ministry of Education and Merit. (2022). *Consolidation and Hardening Programme for Digital Platforms – PRINCE2 Model Applied to Public Administration*. Rome, IT: MIM – Directorate General for Innovation.

CSIRT Italia. (2024). *Incidents and Vulnerabilities in the Italian Public Administration 2023–2024*. Rome, IT: Agency for National Cybersecurity.

About the Author

Luca Paolo Giuseppe Prinzio

Turin, Italy

Luca Paolo Giuseppe Prinzio is a certified Project Manager and Database Administrator at CSI Piemonte in Turin, Italy, where he participates in complex projects on cloud and security. For over twenty years he has worked in the ICT world and carries out teaching and consulting activities in the field of Project Management. He can be contacted at lprinzio@gmail.com and linkedin.com/in/lprinzio

Appendix: Glossary of Acronyms and Abbreviations

Term	Definition
ACN	Agency for National Cybersecurity (Italy). Institution established at the Presidency of the Council of Ministers with tasks of prevention, coordination, and response to national computer incidents.
AgID	Agency for Digital Italy. Technical body defining guidelines, standards, and technical rules for digital transformation and ICT security of the Italian Public Administration.
AI	Artificial Intelligence. Set of computer techniques based on machine learning algorithms and neural networks enabling automated data analysis, pattern recognition, and decision support.
API	Application Programming Interface. Programming interface allowing interaction between different software applications.
BCMS	Business Continuity Management System. Management system conforming to ISO 22301, defining processes and procedures to ensure operational continuity of services even in case of disastrous events or prolonged interruptions.
BIA	Business Impact Analysis. Process assessing operational, economic, and reputational consequences of service interruption.
CAD	Digital Administration Code. Italian legislative decree regulating digitalisation of Public Administration.
CERT-AgID / CSIRT Italia	Computer Emergency Response Team / Computer Security Incident Response Team. National operational structure coordinating response to computer incidents in Public Administration and critical infrastructures.

Term	Definition
CISA	Cybersecurity and Infrastructure Security Agency. US agency developing strategies and guidelines for cyber defence and critical infrastructure protection.
Clusit	Italian Association for Information Security. Independent organisation publishing annual reports on information security trends in Italy.
COBIT	Control Objectives for Information and Related Technology. International ICT governance framework defining control principles and objectives.
CSF	Cybersecurity Framework (NIST). Methodological structure for managing and reducing computer risks, based on Identify, Protect, Detect, Respond, Recover pillars.
CSIRT	Computer Security Incident Response Team. Organisational unit dedicated to managing computer incidents, rapid response, and communication.
DevSecOps	Development, Security and Operations. Methodological approach integrating security into the software development cycle and IT operations.
DPO	Data Protection Officer. Figure required by GDPR ensuring compliance with personal data protection regulations.
DR	Disaster Recovery. Strategies, technologies, and processes for restoring computer systems and data after a disruptive event.
ENISA	European Union Agency for Cybersecurity. EU agency coordinating European cybersecurity policies and supporting Member States in NIS2 implementation.
GDPR	General Data Protection Regulation. European regulation governing personal data processing and free movement within the EU.

Term	Definition
ICT	Information and Communication Technology. Digital technologies and infrastructures supporting information management, processing, and transmission.
IPMA	International Project Management Association. International organisation defining competence standards for Project Managers.
ISMS	Information Security Management System. System conforming to ISO/IEC 27001 for protecting confidentiality, integrity, and availability of data.
ISO	International Organization for Standardization. International organisation defining global standards across various sectors.
ITIL	Information Technology Infrastructure Library. International framework for IT service management.
KMS	Key Management System. Centralised system for managing, distributing, rotating, and revoking cryptographic keys.
MFA	Multi-Factor Authentication. Authentication mechanism based on multiple factors to increase system access security.
ML	Machine Learning. Subdomain of artificial intelligence using statistical models and algorithms to automatically learn from data.
NIS2	Network and Information Security Directive 2. European directive establishing common measures for high-level security of networks and information systems in the EU.
NIST	National Institute of Standards and Technology. US agency developing standards and technical guidelines for critical infrastructure security.

Term	Definition
OPEX / CAPEX	Operational Expenditure / Capital Expenditure. Cost categories: OPEX for recurring operational costs, CAPEX for investments in assets and infrastructure.
PA	Public Administration. Organisational structures of the State and local bodies responsible for providing public services.
PM	Project Manager. Professional responsible for planning, execution, and control of projects.
PMBOK	Project Management Body of Knowledge. Guide published by PMI defining principles, performance domains, and best practices of project management.
PPM	Project Portfolio Management. Integrated system for managing projects and programmes to coordinate priorities, resources, and strategic objectives.
PRINCE2	Projects IN Controlled Environments. Project management method oriented to governance, with principles based on business case, management by phases, clear roles, and exception approach.
PSNC	National Cyber Security Perimeter. Set of Italian infrastructures and subjects considered strategic for national security, subject to cyber protection and surveillance obligations.
RACI	Responsible, Accountable, Consulted, Informed. Responsibility matrix defining roles and involvement levels of project team members.
RPO	Recovery Point Objective. Maximum acceptable data loss (in temporal terms) after an interruption or incident.
RTO	Recovery Time Objective. Maximum time within which a service must be restored after a critical event.

Term	Definition
SLA / SLO	Service Level Agreement / Service Level Objective. Contracts or objectives defining expected service levels.
SIEM	Security Information and Event Management. System for collecting, analysing, and correlating security events in real time.
SOC	Security Operations Center. Operational unit dedicated to continuous monitoring of information security, incident management, and threat response.
WBS	Work Breakdown Structure. Hierarchical structure breaking down the project into manageable components.