Issue 108 | November 2025

NTT DATA

Radar

The Cybersecurity Magazine

NIS2 and DORA: A Unified Governance Framework for Europe

By Carlos Chavarria

The European Union is moving toward a common cybersecurity framework. The update of the NIS2 Directive and the creation of the DORA Regulation aim to unify governance by involving executive-level personnel and integrating risk management, third-party management, incident handling, supply chain security, information security, and business continuity into a comprehensive overarching framework.

These initiatives regulate sectors within the European Union classified as critical under the NIS2 Directive, such as energy, transportation, banking, and healthcare.

Meanwhile, the DORA Regulation standardizes ICT risk management across insurance, capital markets, and banking. Through defined security controls and technical standards, these regulations are helping to harmonize tools, methods, processes, and organizational policies.

All these changes are raising the compliance bar for companies, which in turn is increasing costs to meet regulatory requirements. According to IDC, cybersecurity spending has grown by double digits for two consecutive years — 10.6% in 2023 and 12.3% in 2024.Growth is expected to remain close to double digits through 2026, with the European market projected to reach around USD 71 billion. In parallel, the portion of IT budgets allocated to security has risen to 9.0%, according to ENISA's 2024 report. As a forward-looking indicator, the Infosecurity Europe Trends Report 2025 forecasts an average 31% increase in cybersecurity budgets among surveyed organizations over the next 12 months.

The rise in costs directly translates into improved security measures within organizations — both preventive and reactive. There is now a stronger awareness of the need to strengthen defenses to reduce the likelihood and impact of incidents.

The exponential increase in cyberattacks year after year confirms the importance of having both reactive controls and contingency plans in place, as well as robust incident reporting procedures.

The European Union's plan, through the NIS2 Directive and the DORA Regulation, unifies cybersecurity governance, particularly in how incidents must be reported accurately and within established timeframes.

NIS2 requires extending governance beyond the organizational perimeter, introducing continuous supplier assessments, contractual clauses that cover security controls, and shared continuity plans.

DORA adds the operational dimension for the financial sector: it establishes specific oversight of critical ICT providers, addresses concentration risks, mandates resilience testing, and enforces coordinated incident reporting.

The end result is a single, unified catalog of third-party requirements, a living criticality matrix, and standardized audit evidence.

Third-party management is treated the same way as internal governance, with true due diligence:

- Crisis exercises involving key vendors.
- Health metrics (notification timelines, contractual coverage, and percentage of tested plans).
- Data-driven decisions on dependency.

Implementing these measures leads to fewer surprises and greater measurable resilience.

Europe has chosen its model: regulatory convergence to raise the bar and measure impact with precision. NIS2 and DORA complement each other — the costs increase, but so do the returns:

- Less downtime.
- Reduced legal risk.
- Greater customer trust.

All of this comes together under a single NIS2–DORA governance framework — a unified catalog of controls for business, IT, and third parties, and a timed incident reporting process that closes the loop.

Organizations are moving from compliance for the sake of obligation to demonstrating resilience through data. What was once a box-ticking exercise has evolved into a commitment to continuity protection.

Carlos Chavarría
Cybersecurity Senior Consultant

Ransomware hasn’t gone on vacation.

Cyber chronicle by Antonio Melo and Alejandro Ignacio García

The summer of 2025 has once again shown that cyberspace never stops evolving—or unsettling us. While millions of people were disconnecting, cybercriminal groups and security teams continued their silent, relentless struggle. September marked the end of the summer season with some truly concerning conclusions: a mix of high-impact attacks, critical vulnerabilities, and the beginning of an intense debate around the resilience of critical infrastructures and the role of artificial intelligence in cybersecurity.

Ransomware attacks have maintained their dominance throughout the summer months. Once again, the healthcare sector and public administrations have been the primary targets of ransomware campaigns.

European countries such as Ireland, Switzerland, and Germany have once more experienced system lockdowns that forced some hospitals to suspend appointments or postpone surgeries.

The level of sophistication in these campaigns highlights how criminal groups continue to evolve their hybrid tactics, including double extortion, theft of sensitive data, and public leaks used to pressure their victims.

Zero-days and critical vulnerabilities

The summer brought several urgent security advisories from vendors. Critical vulnerabilities in virtualization systems and widely deployed corporate software forced security teams to apply patches in the middle of August.

The exposure window has once again shrunk to the extreme—reminding us that the patching cycle is no longer measured in weeks, but in hours.

Digital geopolitics under tension

International tensions have also manifested in cyberspace. Recent security research has detected a notable increase in espionage campaigns targeting energy and transport infrastructures in Eastern Europe, linked to state-sponsored actors seeking to gather strategic intelligence amid a climate of growing geopolitical uncertainty.

The offensive and defensive rise of AI

September solidified one of the most debated topics: the role of AI in cybersecurity. As organizations begin experimenting with algorithms capable of detecting anomalies or even automating incident response, attackers are keeping pace. Documented phishing campaigns now use AI-generated messages that are virtually indistinguishable from legitimate communications—raising the level of risk for both users and companies.

Balance: a summer that confirms the trend

This summer’s and September’s cyberchronicle reveal a clear pattern: the professionalization of cybercrime is advancing faster than many organizations can adapt.

Ransomware, zero-days, and espionage campaigns form a cocktail that forces CISOs and security teams to strengthen their anticipatory capabilities. Autumn is shaping up to be a new chapter on a board where the only constant is relentless pressure.

Antonio Melo Leon
Cybersecurity Analyst

Alejandro Ignacio García
Cybersecurity Lead Analyst

GRC: The Strategic Pillar of Organizational Security and Sustainability

Article by Eduardo Fernando Alves

In an increasingly complex digital landscape, organizations face a multitude of risks that extend far beyond technological threats. The interconnection between systems, the dependence on data, and the constant evolution of legislation demand an integrated approach to business management. This is the scenario where the concept of GRC (Governance, Risk, and Compliance) emerges. It is a framework that allows organizations to align strategic objectives, effectively manage risks, and ensure operations comply with standards and regulations.

More than just a set of administrative processes, GRC represents a management philosophy that combines strategic vision, operational discipline, and organizational culture. When properly implemented, it becomes a true competitive differentiator, fostering resilience, transparency, and trust among all stakeholders.

What is GRC and Why It is Essential

Governance, Risk, and Compliance form an inseparable triangle within sound corporate practices. Governance defines how the organization is run, including the decision-making structure, the definition of responsibilities, and alignment with strategic goals.

Risk Management seeks to identify, assess, and mitigate threats that could compromise business continuity, whether they are financial, operational, technological, or reputational in nature. Compliance ensures that all organizational activities conform to laws, regulations, internal policies, and ethical principles.

Integrating these three dimensions is vital to ensuring the company operates responsibly, transparently, and sustainably. When GRC is treated in a fragmented manner, it creates an environment ripe for inefficiency, duplication of effort, and failures that can result in financial losses, reputational damage, and legal sanctions.

The Role of GRC in Cybersecurity is Fundamental

Cybersecurity has transcended the technical sphere; today, it is a strategic priority that permeates the entire organizational structure. An effective Governance, Risk, and Compliance (GRC) program strengthens digital security by establishing clear policies, defining responsibilities, and fostering a culture of continuous vigilance.

With GRC, the company can promptly identify critical cyber risks, assess the potential impact of incidents, and deploy robust response and recovery mechanisms. This alignment with corporate strategy ensures that decisions are guided by real risk, not merely by perception.

Moreover, GRC ensures that security controls do not operate in isolation but are integrated with auditing, regulatory compliance, and business continuity management. It is this holistic vision that separates organizations prepared for the future from those that merely react to crises.

Culture and Leadership: The Foundations of Effective GRC

No GRC program will be effective without the engagement of top management and the commitment of the entire organization.

The risk culture must be fostered from the top, encouraging ethical behaviour, evidence-based decisions, and individual accountability. More than documents and policies, GRC is sustained by people and attitudes.

Internal communication is also a determining factor. When employees understand the value of risk management and recognize their role within that framework, GRC ceases to be viewed as a set of bureaucratic obligations and is instead seen as a tool that supports informed decision-making. Continuous training and awareness are equally crucial.

In the era of digital transformation, risks evolve daily, necessitating teams to be prepared to respond with agility and discernment.

The Benefits of an Integrated Approach

Implementing a mature GRC model brings significant gains to the organization. Key benefits include:

- Improved decision-making, based on consolidated information about risks and controls.

- Reduced costs and duplications through the integration of processes and monitoring systems.
- Increased trust from investors, customers, and regulators due to management transparency.
- Greater operational resilience and capacity to respond to critical incidents.
- Consolidation of organizational reputation as an ethical, responsible, and predictable entity.

Beyond these tangible benefits, GRC promotes responsible innovation.

By understanding its risks and operating in a controlled manner, the company can explore new opportunities safely, without compromising compliance or market trust.

The Real Challenges Behind GRC Implementation Failures

Despite the promises, a significant number of GRC programs do not thrive. The main cause? It's rarely technical.

Most often, the problem lies in disconnected approaches or, worse, the lack of genuine commitment from senior management.

Another common pitfall is suffocating bureaucracy. Some organizations err by adopting excessively complex Governance, Risk, and Compliance frameworks.

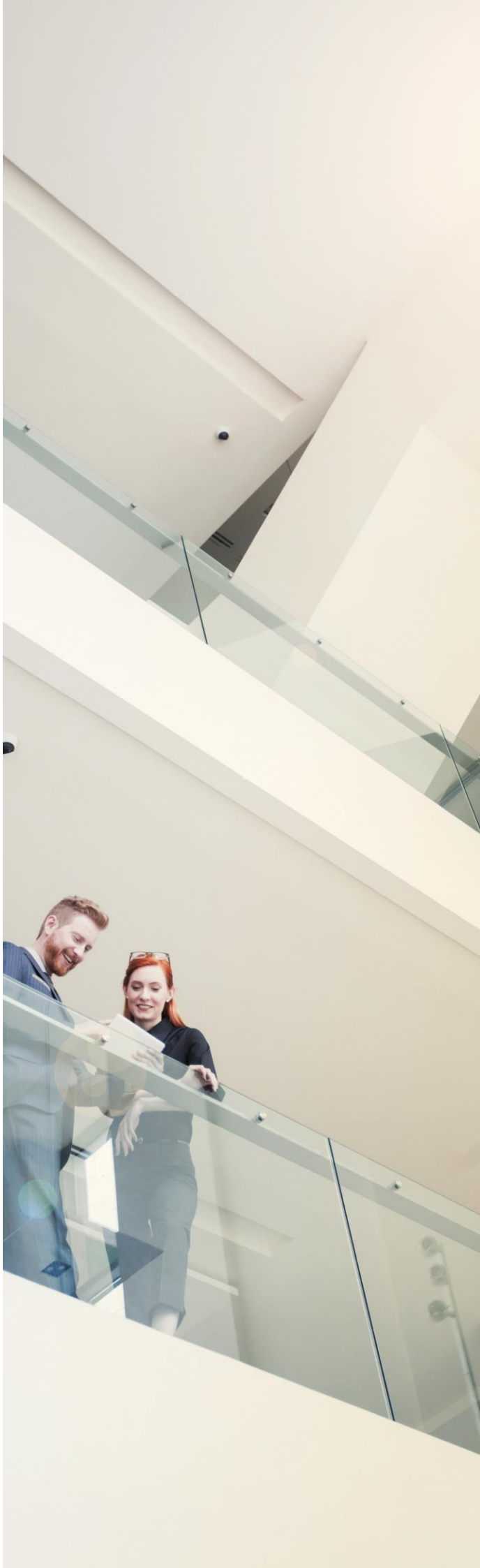
Instead of simplifying operations, they end up creating widespread internal resistance, turning compliance into an obstacle.

The key to a truly effective GRC lies in radical simplification. It is essential to focus on real risk, ensuring that control mechanisms are proportional and perfectly tailored to the company's reality. Technology is a powerful tool, it can centralize data, automate reports, and provide traceability. However, we must not mistake the tool for the objective: technology must always be subordinate to strategy, not the reverse.

The Future of GRC

With the advancement of Artificial Intelligence, automation, and predictive analytics, GRC is entering a new era.

Smart tools are capable of identifying risk patterns, predicting incidents, preparing security assessments, and supporting real-time decision-making.



The trend is for GRC to evolve from a reactive control function into a dynamic, data-driven system that anticipates threats and guides the business proactively.

However, as tools become more sophisticated, ethical and regulatory responsibility also grows.

The future of GRC will require professionals capable of balancing technology, strategy, and human values, always maintaining a focus on integrity and trust.

Conclusion: The Difference Between Reacting and Leading

Governance, Risk, and Compliance (GRC) are not mere corporate obligations. They are, in fact, the foundations that guarantee the credibility, security, and longevity of any modern organization.

We live in an age where cyber threats are interconnected, and regulatory pressure is mounting. In this complex scenario, GRC acts as an essential guide, steering leadership toward responsible and predictable management.

Today, GRC maturity is the true indicator of resilience. Companies that embrace this principle with rigor and strategic vision do not merely avoid penalties; they actively build a solid base for sustainable growth and, most importantly, earn future trust.

Eduardo Fernando Alves
Cybersecurity Expert Engineer

Digital Operational Resilience: Technological Risk, Business Continuity, and Third-Party Risk

Article by Fernando Valles Barbudo

Digital operational resilience is an emerging trend within the management of operational risks across all companies. In the financial sector (banking and insurance), the DORA Regulation (Digital Operational Resilience Act) came into effect this year, representing an additional step forward in the management and control of non-financial risks. Moreover, it can be viewed as a compendium of best practices applicable to non-financial companies that, although not legally required to comply, may wish to rethink their risk management model and risk culture.

Technological Risk

Technology has become a highly significant part of business strategies, moving beyond its former perception as a mere tool.

Its use inherently involves the assumption of associated risks, which makes it essential to have an adequate risk management framework and a clearly defined risk appetite established by senior management. In fact, information and communication technology (ICT) risks can become critical to the survival and resilience of companies.

Moreover, it is not only the risk inherent to an organization's own IT infrastructure that must be considered — the broader ecosystem of impact is much larger. The growing trend of outsourcing infrastructure to hyperscaler-provided services, and their increasingly widespread role in business operations as providers of cloud storage and processing, means that companies not traditionally classified as financial entities have, in practice, become part of the risk analysis flow.

Origins of Technological Risk

The origins of technological risk are diverse, but the following classification is generally used:

- System Availability and Continuity Risk: arises when the development and availability of ICT systems and data are adversely affected. This includes the inability to recover the organization's services in a timely manner due to failures in software or hardware components.
- Information Security Risk: stems from unauthorized access to ICT systems and data, whether originating from within or outside the institution.
- System Change Risk: arises from the institution's inability to manage changes in its ICT systems in a timely and controlled manner.
- Data Integrity Risk: occurs when stored and processed data are incomplete, inaccurate, or inconsistent across different systems, undermining the institution's ability to provide services and manage information accurately and on time.
- Outsourcing Risk: results from the externalization of activities and systems — with particular emphasis on cloud outsourcing.

Events originating from any of these sources can jeopardize business continuity.

Technological Risk as Part of Operational

Operational risk is defined as the risk of (economic) losses resulting from, among other causes:(i) business disruptions and system failures;(ii) execution, delivery, and process management errors;(iii) damage to physical assets; or(iv) fraud (internal or external).Therefore, events that give rise to technological risk must be classified and managed as part of operational risk management. Having an integrated management approach is not merely a technical issue but one of governance — it requires a single risk appetite, a common taxonomy, and priorities aligned with business and process value, rather than being focused solely on the technological component per se.

The process–risk–control triad extends to services, assets, platforms, applications, and vulnerabilities, with both inherent and residual risk needing to be assessed.

Although the management profiles for both types of risk differ qualitatively, both are essential. In the banking sector, these risks can even be incorporated into the estimation of regulatory capital consumption for operational risk.

Critical or Essential Processes

Identifying critical processes is the first step in any resilience strategy. These are the processes whose interruption exceeds the organization's tolerance for business impact. The Business Impact Analysis (BIA) must quantify the Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), Recovery Point Objective (RPO), and all related dependencies — including people, data, applications, infrastructure, and third parties.

It is essential to maintain a living catalog of essential processes, complete with a process–asset–data–provider map and the corresponding quantified risks, both inherent and residual (with and without mitigating controls). This catalog helps prioritize efforts, guide resilience testing, and align all involved teams.

Furthermore, this process map must be bidirectionally linked to the IT components that support operations, enabling risk identification and prevention for compromised systems/processes, vulnerabilities, failures, and other potential disruptions.

Processes classified as critical should be monitored with special rigor, particularly when a third party is involved in the value chain.

Business Continuity and Resilience Testing

Business continuity is not solely defined by ISO 22301. In the banking sector, the DORA Regulation also expands on aspects related to business continuity management.
In addition to proportional strategies derived from the RTO/RPO established in the BIA and the PDCA (Plan–Do–Check–Act) continuous improvement cycle for the Business Continuity Management System (BCMS), DORA establishes several types of resilience testing, including:

- Vulnerability assessments and scansOpen-source analyses
- Network security assessments
- Gap analyses
- Physical security reviews
- Automated scanning questionnaires and solutions
- Source code reviews (where feasible)Scenario-based tests
- Compatibility and performance tests
- End-to-end tests
- Penetration tests (pentesting)

Third-Party risk

Suppliers are an integral part of the operational and digital value chain. Many issues originate from outsourcing to third parties and throughout the entire subcontracting chain. For this reason, effective Third-Party Risk Management (TPRM) is essential and represents one of the core pillars of the DORA Regulation.

In simple terms, vendor management should cover the entire lifecycle, including:(i) Vendor onboarding and approval;(ii) Assessment of the vendor–service relationship;(iii) Service delivery and monitoring; and(iv) Exit or transition strategy.

Control and audit frameworks for operations are evolving, increasingly placing processes at the center and reviewing or auditing them holistically, regardless of who operates them. These frameworks also include all involved teams, whether internal or external.

At this stage, a few key questions arise: How many human and technical resources are dedicated to cybersecurity versus third-party risk? How much actual or potential risk originates from cybersecurity issues compared to third-party dependencies? Is the investment in both areas adequate, proportional, and balanced relative to the risk each represents? Is the company's risk appetite framework sufficiently granular to establish appropriate tolerance levels and identify unacceptable risks that must be mitigated?

Fernando Valles Barbudo
Business Consulting Director – Finance, Risk & Compliance

Quantum Internet

Quantum Space by María Gutiérrez

The “Quantum Internet” is a new generation of communication network that uses the laws of quantum mechanics to transmit information.

While today’s internet is based on copying and transmitting information, the quantum internet relies on something far more radical: the impossibility of copying it. This idea — which might seem paradoxical in the age of digital replication — is, in fact, its greatest strength.

The physical foundation behind it is the no-cloning theorem, one of the cornerstones of quantum mechanics. This principle, formulated in the 1980s, establishes that it is impossible to create an exact copy of an unknown quantum state. In other words, if a particle carries information encoded in its quantum state — for example, the polarization of a photon — any attempt to duplicate or measure it irreversibly alters that state. This inability to copy makes quantum communication theoretically invulnerable to interception.T

oday, the quantum internet is a reality under construction. Functional prototypes and experimental networks exist in various parts of the world. Though the concept may sound abstract, progress is very real.In 2017, the Chinese satellite Micius demonstrated, for the first time, quantum key distribution (QKD) between ground stations separated by 1,200 kilometers. In Europe, the EuroQCI project is building a secure quantum communication network that will link EU member states through terrestrial and satellite connections.

Spain is participating in this initiative through the Quantum Spain program, coordinated by the Institute of Photonic Sciences (ICFO), the Institute for Theoretical Physics (IFT), and the National Cryptologic Center (CCN), which is working on adapting the National Security Framework to the upcoming post-quantum era.

Despite the progress made, the path toward a global quantum internet is filled with challenges.

The first is technological: qubits are extremely fragile and easily lose their coherence, which limits transmission distances. To overcome this, researchers are developing quantum repeaters, devices that could extend the network's range without destroying the information.

The second major challenge lies in infrastructure: quantum networks will not replace existing ones, but rather coexist with them. This coexistence requires hybrid protocols capable of efficiently integrating classical and quantum communications.

Finally, there is a strategic and geopolitical challenge. Quantum communications have direct implications for national security and technological sovereignty. Nations that master these networks will be able to guarantee the confidentiality of their data and protect their critical infrastructures against future quantum-computer-based attacks.

The quantum internet will not emerge all at once, but in phases. First, we'll see metropolitan quantum networks designed for financial or governmental environments, followed by national-scale expansion, and ultimately, a global interconnection. Within one or two decades, the world's most sensitive data — from medical records to diplomatic communications — may be transmitted through quantum channels.

What's fascinating about this revolution is that, once established, it will be invisible to the average user. We'll browse the internet as usual, but beneath the surface, there will exist an entirely new architecture — one designed not only to transmit information, but to preserve it with a level of security we can only imagine today.

The quantum internet does not aim to replace the current one, but to complement it. While traditional networks rely on classical electromagnetism and mathematical cryptography, the quantum network is built on the fundamental laws of nature. It represents not just a technological evolution, but a new paradigm for communication — one in which data protection ceases to depend on algorithms and becomes encoded in the very laws of physics.

Third-Party Risk Management

Trends by Antonio Chavarria

In 2025, 89% of security breaches originate from third-party vulnerabilities, according to the latest Verizon Data Breach Investigations Report. This statistic is more than just a number — it reflects the reality that the traditional security perimeter no longer exists.Modern organizations operate within complex digital ecosystems, where the average number of critical vendors per company has increased by 340% over the past three years. This shift has transformed Third-Party Risk Management (TPRM) from an administrative function into a strategic imperative for business survival.

The convergence of artificial intelligence, regulations such as NIS2 and DORA, and the professionalization of threat groups like Scattered Spider has created a landscape where traditional vendor assessment methods are as effective as medieval armor against a modern cyberattack.

The Revolution of Continuous Monitoring

The old paradigm of annual or semi-annual assessments has collapsed under the exponential speed of evolving threats. Groups like APT40 and Lazarus can compromise a vendor and pivot to secondary targets in under 72 hours, while traditional assessments take 45 to 90 days to complete.

Leading organizations have adopted 24/7 continuous monitoring systems that combine:

- External Attack Surface Management (EASM)Platforms such as Recorded Future and RiskIQ automatically scan vendors' external assets, identifying:
    - Critical vulnerabilities within 4 hours of their public disclosure.
    - Exposed or misconfigured SSL certificates.
    - Undocumented shadow IT services.
    - Accidental database exposures (over 23,000 MongoDB databases were found exposed in 2024).
- Contextualized Threat Intelligence Integration with feeds from Mandiant, CrowdStrike, and Microsoft Defender provides alerts on:
    - Mentions of vendors in ransomware forums such as LockBit 3.0.
    - Suspicious dark web activity involving corporate credentials.
    - Phishing campaigns specifically targeting vendor ecosystems.
- Behavioral Analytics with AI:Machine learning algorithms establish behavioral baselines for each vendor, detecting deviations such as:
    - Anomalous access patterns to critical systems.
    - Undocumented changes in network infrastructure.
    - Sudden increases in data transfer volumes.

Artificial Intelligence — the Engine of TPRM Transformation

Artificial Intelligence is revolutionizing every aspect of the Third-Party Risk Management (TPRM) lifecycle. Generative AI systems can analyze vendor contracts, SOC 2 reports, and technical documentation in minutes instead of hours. Natural Language Processing (NLP) automatically identifies risk clauses, responsibility gaps, and compliance obligations.

The most advanced capabilities include:

- Automatic Questionnaire Generation: systems that create customized assessments based on each vendor's specific risk profile, the type of services provided, and the applicable regulations.
- Predictive Risk Analysis: machine learning models that combine historical data, industry trends, and threat intelligence to predict the likelihood of security incidents.
- Automated Response: AI agents capable of generating draft remediation plans, vendor communications, and executive reports based on assessment findings.

Dynamic and Adaptive Compliance

Regulatory technology (RegTech) is transforming how organizations manage regulatory compliance in their third-party relationships.

RegTech Systems

RegTech systems can track regulatory changes in real time and automatically assess their impact on each vendor relationship, providing:

- Continuous Regulatory Monitoring: systems that automatically track changes in regulations such as GDPR, DORA, and NIS2, and evaluate their impact on existing contracts and processes.
- Automated KYC/AML Assessments: fully automated processes for identity verification, anti–money laundering detection, and sanctions list screening.
- Automatic Generation of Compliance Reports: tools that automatically create regulatory reports with integrated data validation and formatting aligned to specific regulatory standards.

The Future of TPRM

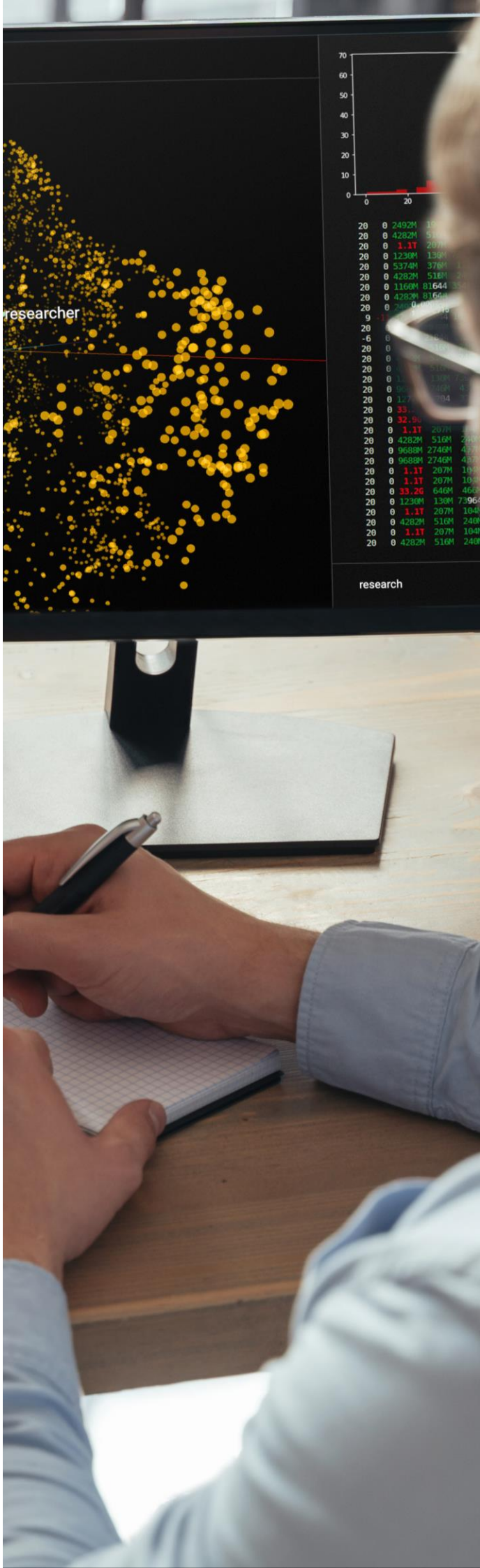
Third-Party Risk Management (TPRM) is evolving toward intelligent ecosystems that combine AI, automation, and predictive analytics to deliver unprecedented risk management capabilities.

Organizations that embrace these emerging technologies will not only strengthen their security posture, but also gain significant competitive advantages in an increasingly interconnected world.

Success in this transformation requires more than just technology implementation — it demands a cultural shift toward proactive collaboration with vendors, investment in advanced analytical capabilities, and executive commitment to excellence in risk management.

Those organizations that lead this evolution will define the future of digital business ecosystems.

Antonio Chavarría
Cybersecurity Senior Consultant



APP Scams in the United Kingdom and Their Mandatory Reimbursement Requirements

Article by Octavio Sánchez Blanco

The United Kingdom has taken the lead in its crusade against scams and, a few months ago, approved regulations under which, in certain circumstances, payment service providers will be required to reimburse the money defrauded. In this article, we analyse the implications of this regulation.

Every year, thousands of individuals and companies fall victim to scams. In this article, we focus on those that are of particular concern to the banking sector due to their high reputational cost and the increase—both in number and amount—observed in recent years. These are known as Authorised Push Payment scams (APP scams).This type of fraud occurs when the victim is deceived into sending money to a scammer posing as a legitimate beneficiary.

There are numerous modus operandi used by fraudsters to trick their victims, but they can generally be grouped into two main categories: “malicious beneficiary” and “malicious redirection.

”In the first case, the victim is deceived into purchasing a product or service that does not exist or will never be delivered; in the second, a scammer impersonates bank staff or technical service personnel (gas, water, technology company) to convince the victim to transfer funds from their bank account to one controlled by the scammer.

The United Kingdom took the lead a few months ago with a regulation targeting this type of fraud, becoming a pioneer in introducing mandatory reimbursement requirements for Authorised Push Payment (APP) scams, which came into force on 7 October 2024.

Announced by the Payment Systems Regulator (PSR) on 7 June 2023, the new rules require UK payment service providers to reimburse all customers who fall victim to APP scams, with only limited exceptions.

In the United Kingdom, the value of authorised payment fraud reached £459.7 million in 2023, across a total of 232,429 cases. The total reimbursement to victims amounted to £287.3 million, representing 62% of the total reported losses (see chart below).Cases: Number of confirmed reported cases. One case corresponds to an account, not an individual.

- Payments: Total number of payments identified as fraudulent in relation to the reported cases.
- Value: Total value of the reported payments.
- Returned to victim: Total amount refunded to the victim, either because the bank directly issued the refund or because the funds were recovered from the beneficiary’s account.

		2020	2021	2022	2023	CHANGE
CASES	PERSONAL	145,207	188,964	200,643	224,694	12%
	NON-PERSONAL	9,407	7,032	6,729	7,735	15%
	TOTAL	154,614	195,996	207,372	232,429	12%
PAYMENTS	PERSONAL	228,946	333,751	361,761	405,095	12%
	NON-PERSONAL	15,625	11,386	10,505	12,364	18%
	TOTAL	244,571	354,137	372,266	417,459	12%
VALUE	PERSONAL	£347.4m	£505.9m	£408.2m	£376.4m	-8%
	NON-PERSONAL	£73.3m	£77.4m	£77.0m	£83.3m	8%
	TOTAL	£420.7m	£583.2m	£485.2m	£459.7m	-5%
RETURNED TO VICTIM	PERSONAL	£163.4m	£246.8m	£254.1m	£256.4m	1%
	NON-PERSONAL	£27.4m	£24.4m	£31.5m	£30.8m	-2%
	TOTAL	£190.8m	£271.2m	£285.6m	£287.3m	1%

Source: Annual Fraud Report 2024. UK Finance

In general terms, the objectives of this implementation in the United Kingdom are:

- To encourage industry-wide investment in end-to-end fraud prevention.
- To enhance customer protection and trust in the payments ecosystem.
- To pursue the PSR's long-term goal of having the UK's interbank payment systems standards body (Pay.UK) take on a broader role and actively improve the rules governing faster payments.

The new requirements will bring about a radical shift in payment culture, strengthening fraud prevention and focusing all companies' efforts on protecting customers.

Agreed Aspects

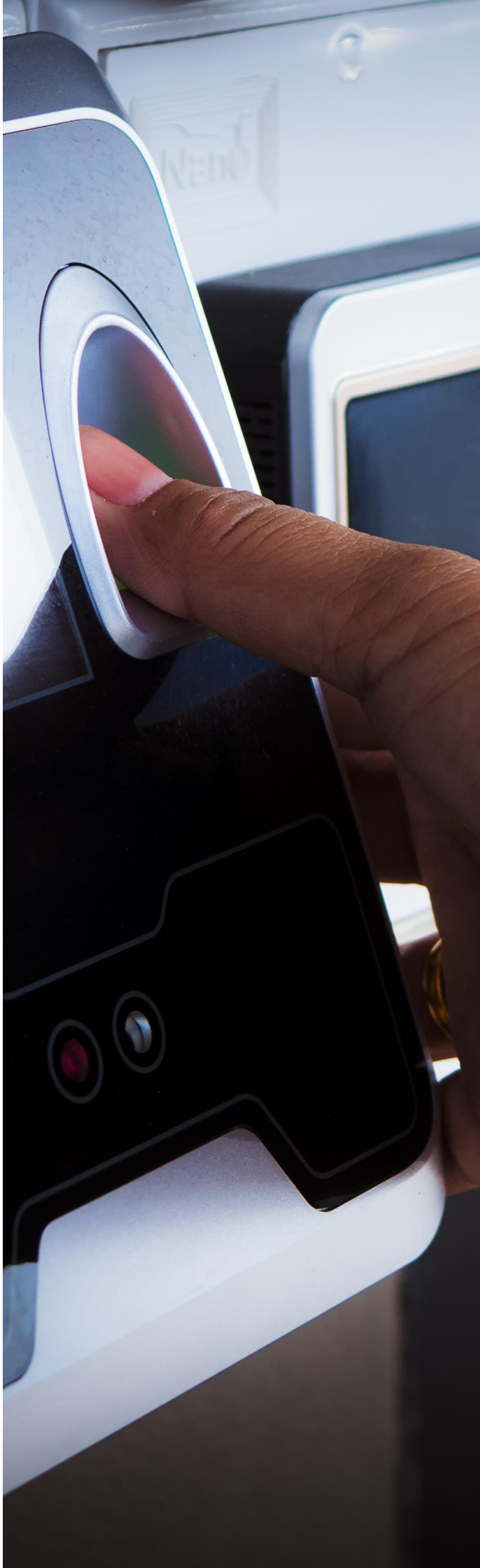
These rules are mandatory for all payment service providers (PSPs) that use the Faster Payments system, covering almost all APP scams.

Reimbursement decisions are made solely by the sending PSP. However, the PSP may claim back 50% of any reimbursement from the receiving payment service provider.

The PSP must issue the reimbursement within five business days, although this period may be extended if further investigation is required (up to a maximum of 35 days).Initially, a maximum reimbursement level of £415,000 was proposed, but this was reduced to £85,000 shortly before the implementation date. The regulator justified this change as a practical adjustment to prevent potential system abuse, emphasising that this new limit would still cover more than 99% of fraud cases.

The new requirements introduce the "consumer standard of caution," which sets out exceptions to the general obligation to reimburse—specifically when the consumer requesting reimbursement has acted fraudulently and/or with gross negligence.

Naturally, the "consumer standard of caution" does not apply to consumers identified as vulnerable to an APP scam.



Reimbursement can only be refused if the customer has failed to meet the "consumer standard of caution" for the reasons mentioned above, and only if the customer is not considered vulnerable. Additionally, the UK Payment Systems Regulator (PSR) has committed to:

- Regularly publishing information on how well firms are protecting their customers.
- Establishing the "Confirmation of Payee" (CoP) system, a name-checking service designed to help prevent scams and misdirected payments.
- Promoting better intelligence sharing among payment firms to detect fraudulent transactions and prevent them from occurring.

There is a 13-month window for submitting claims (although PSPs may voluntarily choose to grant reimbursements for claims submitted after this period).In summary, the United Kingdom is taking action to ensure consumer protection against the growing threat of Authorised Push Payment (APP) scams, aligning with the upcoming implementation of PSD3, whose draft proposal calls for greater focus on customers who may be particularly vulnerable.

By guaranteeing reimbursement in such scam cases, the UK regulator (PSR) aims to push financial institutions to take the initiative in preventing these illicit practices. Collaboration between financial institutions and telecommunications companies will be essential, as will the adoption of new technologies such as behavioural biometrics to improve the detection and mitigation of these scams, which have caused significant reputational damage.

The United Kingdom has been a pioneer with this new regulation. Organisations in other regions will need to pay close attention to the influence this regulation may have on their own national regulators.

The regulator plans to publish a report in the second quarter of 2026. This document will present the results of an independent assessment of the impact of the policies implemented in relation to APP scams, including the reimbursement rules discussed in this article. The evaluation will review the effectiveness and compliance of each policy, as well as the handling of scam cases involving vulnerable customers.

Octavio Sánchez Blanco
FRC FinCrime Leader

Source:
Website of the UK regulator summarising all the organisation's work related to APP scams:https://www.psr.org.uk/our-work/app-scams/Document published by the UK regulator (PSR) on the concept of the "consumer standard of caution":https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdfDocument published by the UK regulator (PSR) on policies to combat Authorised Push Payment (APP) scams: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

Scams: What Are They and What Are the Most Common Types?

Article by Diego José de Benito

The rise in scams has intensified in recent years, creating a sense of insecurity across the population, who feel vulnerable to cybercriminals. In this article, we will introduce the concept of what a scam is, the most common types, and their expected evolution.

A scam is a fraudulent act in which one person deceives another with the intention of obtaining a benefit, usually of a financial nature. In general, scams involve the use of false information to manipulate the victim into making decisions they would not otherwise consider. Scams can take many different forms and methods, ranging from simple deceptions to complex and sophisticated schemes.

It is important to distinguish between a scam and fraud. In the case of fraud, the fraudster uses various techniques to obtain the necessary data for their purpose (financial gain), whereas in a scam, it is the victim themselves who carries out the transaction. Notably, victims of scams generally receive a lower level of protection.

Most common types

Charity, lottery or prize scams

Scammers pretend to represent a charitable organisation (either legitimate or fake) and request donations during times of natural disasters or other emergencies, such as those arising during an ongoing war.

In other cases, scammers inform the victim that they have won a lottery or prize draw, requesting an advance payment to cover the fees or taxes of the supposed reward they are about to receive. In the digital era, technological advancements and society's increasing use and dependence on technology have caused scams to evolve and diversify, turning both individuals and large organisations into clear targets.

In Spain, online scams are the fastest-growing type of crime, increasing by 509.1% between 2016 and 2023. In the first quarter of 2024, one in every seven crimes fell into this category.

Fake job scams

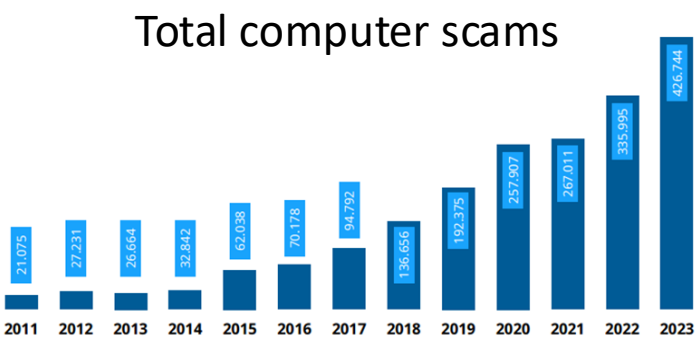
Nowadays, job scam attempts are extremely common on platforms such as WhatsApp or LinkedIn, often involving supposed employment opportunities where the scammer pretends to work in the payroll or administration department of a well-known company or organisation.

These offers usually promise remote work, minimal effort and time commitment, high flexibility, and an attractive salary. Later, the scammers request "processing fees" to send work equipment or use another excuse to get the victim to make an advance payment in exchange for the remuneration of the supposed job.

Investment scams

Investment scams are among the most common today, driven by the rise of social media and online investment platforms or apps, where scammers have found new ways to reach large numbers of potential victims with promises of instant wealth or high investment returns.

Scammers use different strategies, in addition to promising great profits, such as Ponzi schemes—in which returns are paid to earlier investors using the funds of new ones—or pyramid schemes, which encourage victims to recruit more people to maintain the flow of profits. Failure to recruit often means losing the initial investment.



Crime Report – Ministry of Interior

Sometimes, victims are asked to install a remote control application on their devices, such as AnyDesk, under the pretext of teaching them how to carry out investment operations. In reality, the scammers end up taking control of these devices and performing fraudulent transactions without the victim's knowledge. For specific investment profiles, scams related to pump-and-dump schemes (artificially inflating the price of a stock or asset through false or misleading information), binary investments, micro-cap investments, or investment seminars are commonplace.

TOP 5 INVESTMENT SCAMS

- Ponzi scheme
- Pump-and-dump schemes
- Pyramid schemes
- Advance fee fraud
- Options scams

A special mention, due to their exponential growth, goes to cryptocurrency investment scams or affinity group scams (e.g., Forex investment).

Technical Support Scams

Also known as the "Microsoft scam," this type of fraud exploits the lack of technological knowledge among certain sectors of the population. Scammers contact victims via phone calls or emails, warning them of a supposed security issue on their device that requires immediate intervention to prevent further problems. They then request personal and sensitive information from the victim through social engineering techniques in order to gain remote access to the device.

Commercial Scams

These are among the oldest scams in existence, practically dating back to the beginnings of commercial transactions. Nowadays, they can occur through insecure e-commerce platforms, auction websites, and are very common on social media. In recent times, they have become especially frequent on online marketplaces and second-hand selling apps such as Wallapop or Vinted.

These are fake advertisements through which the victim makes advance payments for goods or services they will never receive or that do not actually exist. The products and/or services involved in this type of scam are highly varied and can change depending on the time of year.

Examples include scams related to holiday rental properties, pellet (heating fuel) purchases, automobiles, pet adoptions, and more.

Romance Scams

Scammers use platforms such as social networks or dating apps/websites to create attractive profiles with fake photos and biographies to lure potential victims. In some cases, they even impersonate celebrities or well-known public figures. It is very common for them to pose as military personnel stationed abroad.

This type of scam often unfolds over a long period of time, as the fraudsters establish a strong emotional connection with the victim through frequent communication, affection, and seemingly genuine interest in their life.

Once they have gained the victim's full trust, they typically claim to have a health issue, a financial emergency, travel expenses, or visa problems that prevent them from meeting in person. They always try to apply pressure using false emergency situations that make the emotionally involved victim overlook the suspicious nature of the request.

It is alarming how some victims can end up losing large sums of money—sometimes their entire life savings—while also suffering deep emotional distress, shame, and humiliation, which in turn increases their sense of loneliness and isolation.

Estafas de Suplantación de un Organismo Oficial o Empresas de Servicios

El estafador se hace pasar por una de estas organizaciones mediante llamadas, correos electrónicos o SMS alertando de una supuesta deuda con Hacienda, con la compañía amenazando de un corte inmediato de luz, agua, paquete que no va a ser entregado... y solicitando movimientos directos por parte de la víctima.

IBAN Manipulation / Invoice Fraud

This type of scam is most commonly targeted at companies, although individuals can also fall victim to it. Through social engineering techniques, scammers obtain information or the email address of a company's regular supplier or service provider. They then intercept or alter a digital or physical invoice to change the bank account details, ensuring that the next payment is redirected to their own accounts.

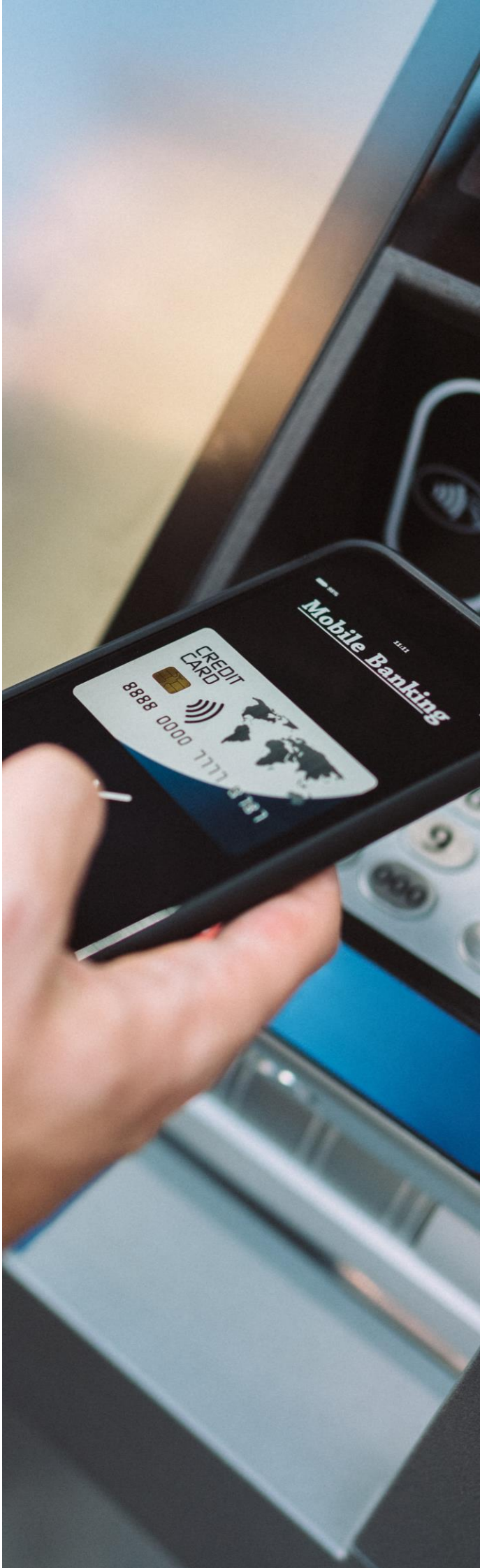
Typically, the amount and timing of the fraudulent invoice match those of previous legitimate transactions with the impersonated company, which makes the deception harder to detect.

Bank impersonation scams

The impersonation of a bank employee is a type of fraud that has been growing rapidly. Scammers often make contact by phone, sometimes already possessing personal information about the victim obtained through other social engineering methods.

They present themselves as account managers or members of the bank's security department, mimicking the behavior of real employees. They inform the victim of supposedly suspicious activity on their account or of an unauthorized transaction, generating anxiety, urgency, and concern. Under the pretext of taking immediate action to protect their money, they eventually convince the victim to hand over online banking credentials, share two-factor authentication codes to "confirm" operations, or even initiate transfers directly to the fraudster's account.

Scammers frequently use a technique known as spoofing, which makes their calls appear to come from legitimate phone numbers belonging to the bank—often customer service lines.



Impersonation of a Family Member

Very common through WhatsApp, this type of scam has surged in recent years. It usually takes the form of a message from someone pretending to be a child studying abroad or traveling, who claims to be in a sudden emergency and therefore contacting the parent from an unfamiliar number. Sometimes, scammers use specific information about the victim's child that they have gathered from social media.

Appealing to the family member's concern, they insist on the urgency of the situation and claim that any delay in sending the requested amount will have serious consequences. They typically demand immediate money transfers that are impossible to reverse once the victim realizes they've been deceived.

Money Mule Recruitment Scams

These scams often begin in a similar way to fake job offers. Fraudsters advertise legitimate-looking job opportunities or reach out directly to individuals via social media, but their real goal is to convince them to act as intermediaries—opening a bank account for this purpose or using their existing one—to transfer money they believe to be legitimate. In many cases, victims are unaware that they are committing a crime.

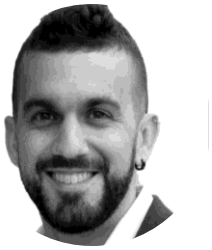
The network of money mules enables the laundering of funds obtained from other scams or frauds through real-time payments, quickly moving money between multiple accounts to make it difficult to trace.

CEO fraud

In this type of scam, a criminal or a group of criminals, through various social engineering techniques, manages to impersonate the CEO of an organization. The modus operandi consists of convincing an employee responsible for the organization's accounts or financial transactions to urgently transfer money to the scammer's account.

This type of fraud typically targets companies and is often carried out through communication channels such as WhatsApp, SMS, or internal corporate chat tools like Microsoft Teams.

As we have seen, the range of scam typologies is extremely broad and constantly evolving. Because of this, the exponential growth in both the variety and volume of attacks requires continuous investment in resources that help protect consumers. Moreover, it also demands proper fraud prevention management to reduce potential regulatory penalties.

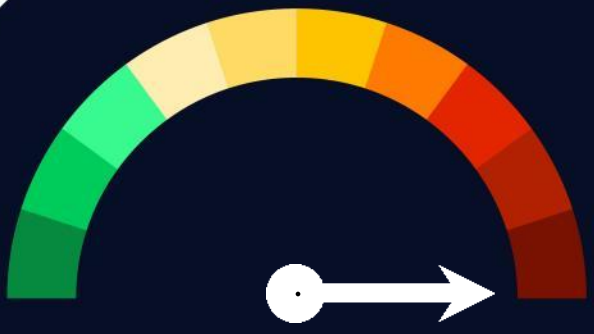


Diego José de Benito
FinCrime Analyst
Financial Risk &
Compliance (FRC)

Vulnerabilities

Critical Vulnerability in Redis

Date: October 3, 2025
CVE: CVE-2025-49844



CVSS: 9.9

CRITICAL

Description

The vulnerability CVE-2025-49844 (nicknamed "RediShell") represents a critical threat, as it allows attackers to achieve remote code execution on thousands of vulnerable instances. It is a use-after-free (CWE-416) flaw that has been present in Redis's source code for more than a decade.

In this context, an attacker with valid credentials could use a specially crafted Lua script (a feature enabled by default) to escape the sandbox, trigger the memory error, establish a persistent reverse shell, and ultimately execute remote code on the affected system.

Solution

Redis recommends updating to version 8.2.2, especially for instances accessible from the Internet.:

- An additional workaround to mitigate the issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done by using ACLs to restrict the EVAL and EVALSHA commands

Affected products

This critical vulnerability affects versions 8.2.1 and earlier, which allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free condition, and potentially lead to remote code execution.

References

- nvd.nist.gov
- bleepingcomputer.com

Vulnerabilities

Critical vulnerability in Flag Forge

Date: October 10, 2025
CVE: CVE-2025-617777

CVSS: 9.4

CRITICAL

Description

A critical vulnerability has been identified in Flag Forge, a platform used for Capture The Flag (CTF) competitions.

The flaw is located in the administrative endpoints /api/admin/badge-templates (GET) and /api/admin/badge-templates/create (POST), which allowed access without authentication or authorization.

This vulnerability, with a CVSS score of 9.4, could be exploited by a remote unauthenticated attacker to retrieve all badge templates containing sensitive data, as well as to create arbitrary templates directly in the database.

Solution

It is recommended to immediately update to version 2.3.2, in which the vulnerability has already been fixed.

Affected products

The vulnerability affects the following products:

- Forge CTF Platform:versions 2.0.0 to 2.3.1

References

- incibe.es
- github.com

TLP:WHITE

Oracle fixes a zero-day vulnerability in Oracle E-Business Suite

Date: October 5, 2025
CVE: CVE-2025-61882

Critical

Description

Oracle has released an urgent patch for a zero-day vulnerability in its E-Business Suite (EBS), identified as CVE-2025-61882, which has been actively exploited by the Clop group in data theft attacks.

According to Oracle, this weakness resides in the "BI Publisher Integration" component of the EBS "Concurrent Processing" module.

The most serious aspect is that it does not require authentication: an attacker can exploit it over the network without a username or password, allowing remote code execution if the attack is successful.

The vulnerability has a base CVSS score of 9.8, reflecting its criticality given the ease with which it can be exploited and its potential impact.

Affected Products

Oracle has confirmed that the zero-day vulnerability affects the Oracle E-Business Suite product, from version 12.2.3 up to version 12.2.14.

Solution

Oracle has released an emergency update to address the flaw; however, in order to install the emergency patch for CVE-2025-61882, the October 2023 Critical Patch Update must first be applied.

References

- nvd.nist.gov
- bleepingcomputer.com

IBM fixes vulnerabilities that allow privilege escalation

Date: October 9, 2025
CVE: CVE-2025-36356 and 2 more

Critical

Description

IBM has published a security bulletin to address multiple vulnerabilities in IBM Security Verify Access and IBM Verify Identity Access products.

The most severe (CVE-2025-36356) allowed a locally authenticated user to escalate their privileges to root level due to execution with excessive permissions. This vulnerability has a CVSS score of 9.3.Additionally, other flaws have been fixed that could have allowed unauthorized command execution or the inclusion of code from external environments.

Affected products

The products affected by the update are as follows:

- IBM Security Verify Access (Docker and Appliance): versions 10.0.0.0 to 10.0.9.0-IF2
- IBM Verify Identity Access (Docker and Appliance): versions 11.0.0.0 to 11.0.1.0

Solution

IBM recommends updatin the affected products to the patched versions:

- IBM Security Verify Access: apply Fixpack 10.0.9.0-IF3
- IBM Verify Identity Access: apply Fixpack 11.0.1.0-IF1

References

- ibm.com
- incibe.es

Events

XIX Jornadas STIC CCN-CERT | VII ESPDEF-CERT Cyberdefense Conference | RootedCON Congress

24 - 27 November

The largest national cybersecurity event will take place at the Kinépolis Ciudad de la Imagen cinemas in Madrid under the motto "A Digital Shield for an Interconnected Spain." For the first time, the National Cryptologic Center (CCN), the Joint Cyber Command (MCCE), and RootedCON are joining forces to create an integrated program that will bring together over 7,000 professionals.

The event will kick off on November 24 with a special edition of the RootedCON Congress focused on training and hands-on sessions. From November 25 to 27, the main conference will feature the latest research, policies, and cybersecurity protection technologies.
Link

IT & Cybersecurity Meetings Marbella

18 – 20 November

An innovative one-to-one fair dedicated to networking, cloud, mobility, cybersecurity, and AI solutions will be held at the Marbella Congress Center (Málaga). The event features a unique concept of 15-minute pre-scheduled business meetings between qualified decision-makers from France, Italy, Germany, and Switzerland and international exhibitors.

The fair will bring together over 80 exhibitors and 150 decision-makers, with networking opportunities through cocktail dinners that allow business development to continue in a relaxed atmosphere.

Link

ISMS Forum Spain

13 November

The twenty-seventh edition of the International Information Security Conference will take place at the Cívitas Stadium, organized by ISMS Forum. It focuses on information systems management and security regulations.

Link

Real-Time Cybersecurity: From Alert to Action

20 November

Ayesa is organizing this specialized event from 10:00 AM to 2:00 PM in Madrid, focused on immediate threat response and the transition from detection to corrective action.

Link

Resources

➢ Check Point Infinity AI Security Services: Intelligent Threat Detection

Check Point Infinity has been recognized as the best AI-powered cybersecurity platform according to Miercom's 2025 report. This unified architecture provides comprehensive protection for networks, cloud, endpoints, and mobile devices, leveraging 50 AI engines that analyze big data from millions of connected devices.

Its ThreatCloud system integrates advanced threat intelligence with Zero Trust and Secure Access Service Edge (SASE) capabilities, offering ease of use and centralized security management.

Link

➢ AccuKnox AI CoPilot: Security Assistant for Cloud Environments

A new tool specifically designed to protect serverless applications, containers, and Kubernetes environments using generative AI. AccuKnox leverages eBPF technology for deep system monitoring, identifying risks, developing security policies, and efficiently managing incidents.

This platform stands out for its focus on cloud-native security without compromising existing operations, providing early threat detection and automated response.

Link

➢ Darktrace ActiveAI Security Platform: autonomous threat detection

Darktrace has evolved its platform to detect threats by learning normal network behavior, without relying on known attack signatures. Its autonomous response capability, Antigena, can contain attacks in a targeted manner without disrupting business operations.The platform uses behavioral analysis to identify high-risk anomalies, including sophisticated AI-driven threats, establishing unique models for each digital business environment.

Link

➢ SentinelOne Singularity: Unified protection with behavioral AI

SentinelOne Singularity integrates unified protection, detection, and response for endpoints, cloud workloads, and identities. Its behavioral AI can stop ransomware, zero-day threats, and active attacks using static and behavioral models that operate across operating systems and cloud environments.

The platform includes Purple AI for natural language threat search, automatic summary generation, and investigation acceleration, along with automated policy-based response.
link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com