The New Imperative: Cyber Resilience

In today's landscape, cyber attacks are an inevitability. The focus must shift from pure prevention to holistic resilience—the ability to anticipate, withstand, recover, and adapt.

98%

of common attacks can be prevented by implementing five minimum security standards.

Microsoft's 5 Minimum Standards

Enable Multi-Factor Authentication (MFA): A fundamental control to protect identities against compromised passwords.

Apply Zero Trust Principles: Never trust, always verify. Limit impact by assuming breach and using least privilege access.

Use Modern Anti-Malware: Employ XDR solutions to automatically detect and block advanced threats.

Keep Systems Up to Date: Regularly patch all systems and applications to close known vulnerability windows

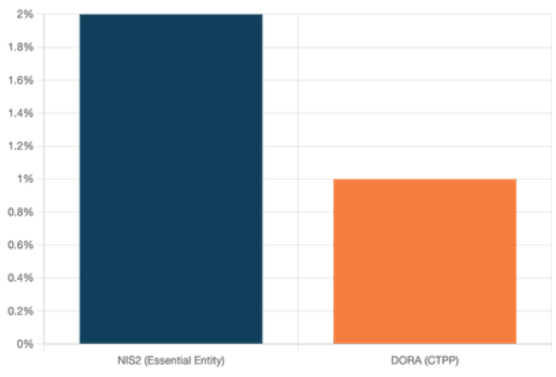
Protect Your Data: Know where your critical data is and implement robust protection and backup systems.

Navigating the EU Regulatory Maze

The EU has introduced two pivotal regulations, DORA and NIS2,to fortify digital operational resilience. While complementary, they have distinct scopes and requirements.

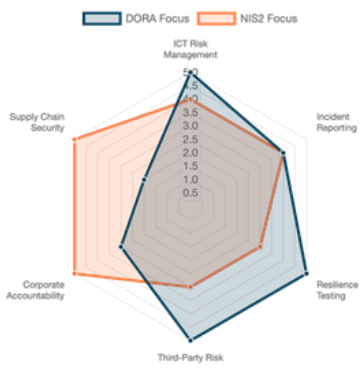
Comparing Maximum Financial Penalties

NIS2 imposes significant fines based on global turnover, while DORA's penalties for Critical Third-Party Providers (CTPPs) are calculated on daily turnover, potentially accumulating rapidly.



Core Compliance Pillar Focus

Both frameworks emphasise core security principles, but with different areas of focus. DORA is highly prescriptive about third-party risk and resilience testing, while NIS2 places a strong emphasis on corporate accountability and supply chain security.



Incident Reporting Timelines

Both DORA and NIS2 mandate a strict, multi-stage incident reporting process. Failure to meet these deadlines is a primary cause of non-compliance penalties.

24 Hours — Initial Notification / Early Warning → **72** Hours — Detailed Report / Impact Assessment → **1** Month — Final Comprehensive Report

Your Compliance Toolkit: M365 in Action

Microsoft 365 provides a powerful suite of integrated tools that map directly to the core requirements of both DORA and NIS2, forming the foundation of your compliance strategy.

Identity & Access Management

Secure access to resources and enforce least privilege.

Microsoft Entra ID

Data Governance & Protection

Classify, protect, and govern sensitive data everywhere.

Microsoft Purview

Threat Detection & Response

Detect, investigate, and respond to threats in real-time.

Microsoft Sentinel & Defender

Endpoint & Device Management

Ensure all devices accessing corporate data are secure and compliant.

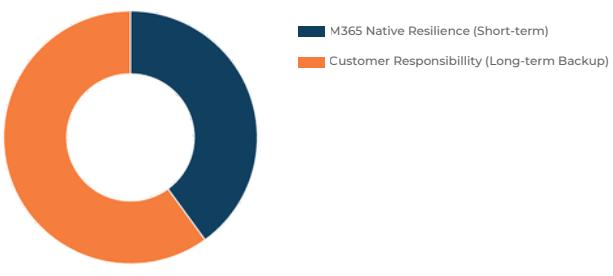
Microsoft Intune

The Shared Responsibility Gap

While Microsoft provides robust "security-of-the cloud," your organisation is ultimately responsible for "security-in-the cloud." A critical gap often exists in data backup and long-term retention.

The Backup & Retention Gap

Microsoft's native features provide excellent short-term resilience (e.g., recycle bins). However, DORA and NIS2 require long-term, immutable backups for comprehensive data recovery and compliance, which often necessitates third-party solutions.



Division of Responsibilities

Microsoft's Responsibility (Security OF the Cloud)

- Physical Data center Security
- Network Infrastructure Host
- Operating Systems
- Application-level Controls

Your Responsibility (Security IN the Cloud)

- Data Classification & Accountability
- Endpoint Protection & Configuration
- Identity & Access Management
- Comprehensive Data Backup & Recovery
- Overall Regulatory Compliance

A Practical Roadmap to Resilience

Achieving compliance and true cyber resilience is a continuous journey. Follow these 5 essential steps to build a robust and adaptive security posture with Microsoft 365.

1. **Implement Universal MFA**
   Protect all user accounts from credential theft. This is your single most effective security control.
2. **Enforce Least Privilege**
   Use PIM and Conditional Access to grant only the minimum necessary permissions, just in time.
3. **Establish Regular, Immutable Backups**
   Deploy a third-party solution for comprehensive, long-term, and tamper-proof backups of all M365 data.
4. **Develop & Test an Incident Response Plan**
   Document your response procedures and use tools like Sentinel to automate and accelerate them.
5. **Conduct Continuous Monitoring & Audits**
   Use Defender for Cloud and regular penetration testing to proactively identify and remediate weaknesses.

Elasticito | 128 City Road | London | EC1V 2NX | United Kingdom | +44 3330428268