veeam

Demystifying Regulatory Compliance

Standards, frameworks and recommendations

Introduction

The development of regulatory frameworks and standards has emerged from the need to address the challenges and requirements in managing information technology and safeguarding data. These frameworks and standards have not only evolved over time, but they have been shaped by technological advancements and emerging cybersecurity threats.

The evolution of frameworks and standards has been primarily driven by the following factors:

- **Regulatory bodies** emphasize the need for organizations to be accountable for their cybersecurity practices and to comply with specific standards and regulations.
- **Advanced cyberthreats** are more frequent and damaging. They were once confined to sophisticated state-sponsored threats but are now in the hands of opportunists and hacktivists.
- **Critical infrastructure and essential services** (e.g., healthcare, energy, finance) that are vital to the functioning of society and the economy. This includes federal legislation, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) of March 2022.
- **A lack of uniformity** in cybersecurity practices across different sectors and regions. Inconsistent approaches can lead to gaps in security and compliance challenges.

Organizations need to be resilient in the face of cyberthreats and ensure they can continue to operate and recover quickly from disruptions. With the growing amount of personal data being collected and processed, there is a heightened need to protect this data from cyber threats and data breaches. Cyber incidents not only have a significant economic impact, leading to financial losses and undermining trust in digital services for the broader economy, but in some cases can cost lives, especially where the healthcare industry has been targeted.

Meeting compliance is crucial for building organizational resilience. Organizations that grasp the full scope of their risks recognize that adhering to frameworks and standards as well as meeting regulatory compliance isn't just a checkbox activity, but a fundamental part of an overall security strategy improving their security posture and in a better position to withstand and quickly recover from most cyberattacks. This approach ensures resilience, if a crisis hits, the groundwork for rapid recovery is already in place.

Regulations vs. Frameworks

The core difference between regulations and frameworks is what you are trying to accomplish. Frameworks provide the foundation for compliance with regulations, and regulations drive the adoption of frameworks to manage and improve their cybersecurity posture. Differently, regulations are legal requirements imposed by governments or regulatory bodies to enforce a minimum standard of cybersecurity practices across organizations. Some widely used regulations include:

- **GDPR** (General Data Protection Regulation) — European Union regulation for data protection and privacy.
- **DORA** (The Digital Operational Resilience Act) — European Union regulation mandates that financial entities maintain resilient Information and communication technology (ICT) systems, including secure data backups and recovery procedures.
- **NIS2** (Network and Information Security Directive) — European Union Directive introduces mandatory cybersecurity measures like risk management, supply chain security, and incident response plans.
- **CIRCIA** (Cyber Incident Reporting for Critical Infrastructure Act of 2022) — U.S. federal law mandates that critical infrastructure organizations report significant cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA).
- **HIPAA** (Health Insurance Portability and Accountability Act) — U.S. regulation for protecting healthcare information.
- **SOX** (Sarbanes-Oxley Act) — U.S. regulation for financial practices and corporate governance.
- **PCI DSS** (Payment Card Industry Data Security Standard) — Standards for securing credit card transactions.
- **FISMA** (Federal Information Security Management Act) — U.S. law for protecting government information.

Regulations like these work in tandem with frameworks. For example, frameworks provide the foundation for compliance with regulations, and regulations drive the adoption of frameworks. Frameworks also help organizations go beyond minimum regulatory requirements and facilitate easier compliance and auditing while regulations ensure consistent baseline security across sectors. Some widely used frameworks include:

- **NIST Cybersecurity Framework (CSF)** — Provides a comprehensive approach to managing cybersecurity risks.
- **CIS Controls** — A set of best practices to defend against cyber threats.
- **ISO/IEC 27001:2022** — An international standard for managing the security of information assets to ensure the confidentiality, integrity, and availability of corporate data.
- **SOC 2** — To assess the effectiveness of a service organization's controls over sensitive customer data and systems.

- **COBIT** — Provides a framework for IT management and governance, with a strong focus on control objectives for IT, including cybersecurity.
- **ISO 22301** — Provides a framework for organizations to prevent, prepare for, respond to, and recover from disruptive events like cyberattacks, natural disasters, and supply chain failures.

Why Compliance Matters

Compliance involves adhering to laws and regulations that apply to the organization's industry and geography. Being complaint helps reduce the impact to your business, from loss of revenue due to ransom payments to operational disruption, data breach exposures, regulatory fines, and reputational damage. Compliance standards are changing rapidly and will continue to do so. Regulations developed today to meet current objectives may not work in the future. Keeping up with the new frameworks and regulations and their new expectations is a surefire way to protect your organization.

Compliance Recommendations for IT and Security Teams

Compliance is far from a one-time consideration. Requirements are not static and evolve over time as new threats emerge and regulations are updated. As such, there are some best practices and particular requirements organizations must pay attention to.

1 Minimum Security Posture Requirements for Data Protection

Standards, frameworks, and regulators rarely dictate which technology you must deploy, but security controls like encryption, access management, and audit logging are expected to meet compliance. A baseline of security measures is a must for internal audits as well as external compliance. Here are a few examples:

- CIS Controls v8 controls 3,4, 5, and 6 cover safeguards for Data Protection, Access Control Management, Account Management, and Privileged Access Management
- NIST CSF 2.0 framework — PR.DS for Data Security & PR.AC for Access Control address confidentiality, integrity, and availability (CIA) requirements of data protection, including encryption, key management, and authorization, amongst other recommendations.
- GDPR Article 32 references data encryption and the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- PCI-DSS v4.0 dedicates multiple requirements to strong cryptography, mandatory multi-factor authentication (MFA), audit logs, ongoing security monitoring, and testing.

RECOMMENDATIONS:

Meeting a "minimum security posture" isn't optional. Standards, frameworks, and regulators outline the same fundamentals. Use them to justify budget for encryption, identity management systems, data protection platforms, to implement Zero Trust principles, and SIEM technologies.

2 Backup & Recovery: The Last Line of Defense (and Compliance)

Backups and tested recovery are not just a best practice; they're a compliance mandate. Almost every standard requires steps to achieve data resilience. If your organization is doing it across all digital infrastructure, it's already meeting compliance but find out more about every requirement.

- **The** NIST SP 800-209 security guidelines for storage infrastructure security including backup isolation, restoration, and encryption.
- **ISO/IEC 27040 standard** on storage security provides detailed guidance on organizational, human, and technological controls needed to secure data in systems.
- **ISO 27001:2022** — Annex A 8.13. Information backup, is a security control that requires organizations to maintain and test backup copies of essential information.
- **PCI-DSS v4.0** — Requirement 12.10.1: Mandate to establish cyber-incident response plans with data recovery and continuity procedures.
- **The Digital Operational Resilience Act (DORA)** mandates that financial entities maintain resilient Information and Communication Technology (ICT) systems, including secure data backups and recovery procedures

Increasingly, compliance requirements are explicit about how to backup data: immutable media (air-gapped, worm-locked, or object-lock), regular validation, and access controls so threat actors can't reach backups and prevent recovery.

RECOMMENDATIONS:

Require immutable, air-gapped backups. Separate backup repositories from production environments. Test recovery regularly and enforce zero trust principles for data protection. Learn more about Veeam's 3-2-1-1-0 rule for secure backups. Remember that it's not just backups, it's about testing recovery and documenting processes.

3 Third-Party Risk: The Supply Chain Attack Surface

Supply chain attacks have become one of the most insidious vectors for ransomware. Threat actors now target the weakest vendor in a chain to gain legitimate access and then launch a cyberattack. Organizations operations are increasingly dependent on third-party vendors and software. A strong security posture must include action to mitigate risk from the supply chain. Fortunately, most compliance drivers include recommendations or requirements including:

- SOC 2 Trust Services Criteria (TSC): Includes vendor management controls including protection from unauthorized access.
- NIST SP 800-161 Supply Chain Risk Management provides guidance on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organization.
- PCI-DSS v4.0, requirements 12.8.x mandates card-processing organizations to maintain a vendor management program that includes written agreements and continuous oversight.
- ISO 27001:2022 — Annex A 5.19 is about information security in supplier relationships and lists security controls.
- DORA in the EU requires financial entities to map and assess all ICT third parties to manage risks through their supply chain.
- NIS2 Directive in the EU expands obligations to include supply chain risk.

RECOMMENDATION:

Regardless of the industry and regulation, validating vendors' security practices should be table stakes. Questionnaires, SOC 2 reports, continuous monitoring tools, maintaining up to date inventories, software bill of materials (SBOMs), and enforcing zero-trust access principles goes a long way on protecting from supply chain ransomware attacks.

4 Minimum Viable Business (MVB): Prioritizing What Matters Most

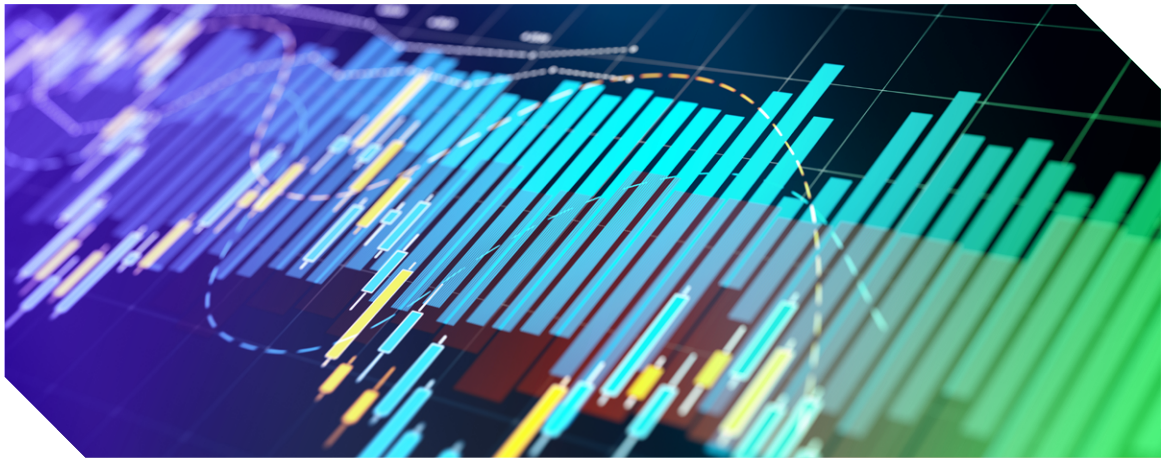
In the event of a cyberattack including ransomware encryption or even corruption of data it is important for organizations to include in their incident response plans documentation that defines the concept of Minimum Viable Business (MVB) or Minimum Viable Company (MVC). It refers to identifying the minimum essential systems and processes needed to keep operations running after a cyberattack. Prioritizing digital infrastructure goes a long way in the moment of crisis.

Standards and frameworks have similar language — often labeled Business Continuity Management (BCM) or Impact Analysis for example:

- **ISO 22301, Business Continuity Management** works alongside ISO 27001 to establish business impact analysis, minimum levels of operation, and recovery time objectives for business processes.
- **ISO 27001 Information Security Management** requires organizations to identify critical business processes, information assets and supporting systems.
- **NIST SP 800-34 Contingency Planning Guide** provides detailed guidance on contingency plans identifying critical business functions, establishing recovery priorities, and defining minimum operational capabilities during cyberattacks, natural disasters, or system failures.
- **DORA entities** must develop and maintain a formal ICT business continuity policy, approved and regularly reviewed by senior management.

RECOMMENDATIONS:

Map dependencies from applications down to supporting infrastructure, let security teams focus resources where downtime costs the most. MVB isn't about doing less security; it's about doing security right the first time while the goal is for all systems and data to be restored.



5 Incident Reporting Regulations

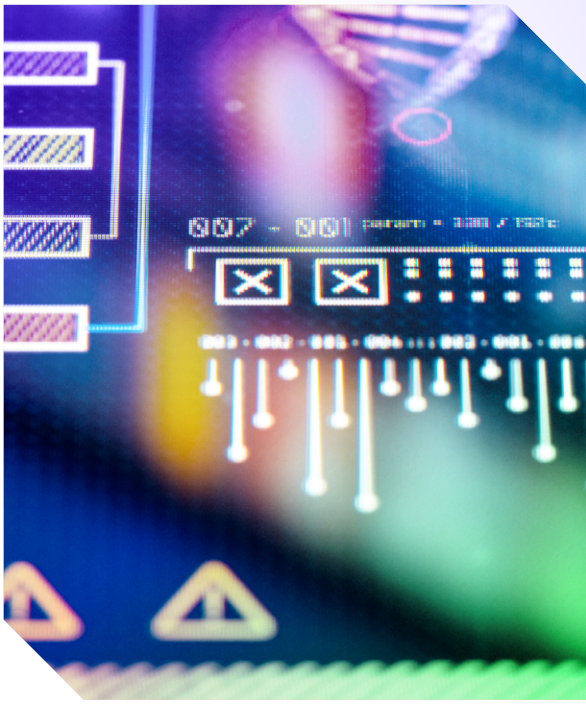
Many countries are adding regulations to demand transparent cyberattack reporting. In the US, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), requires reporting a cyberattack within 72 hours, and ransom payments within 24 hours. Similar regulations have passed in multiple countries across the world:

- **EU NIS2 Directive** expanded incident reporting requirements to a broader range of critical and important sectors. It mandates to report significant cybersecurity incidents within 24 hours.
- **GDPR Articles 33-34:** requires notification of data breaches no later than 72 hours.
- **SEC Cyber reporting rules** mandate public companies to disclose material cybersecurity incidents within four business days on a Form 8-K.
- **UK GDPR:** requires organizations to report personal data breaches within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals.
- **Australian Prudential Regulation Authority (APRA) standard CPS 234** requires regulated entities to notify APRA as soon as possible, and no later than 72 hours after becoming aware of a material information security incident.
- **Singapore's Personal Data Protection Act (PDPA):** Organizations must notify of a data breach if it results in, or is likely to result in, significant harm to an individual, no later than three calendar days from the day the organization determines the breach is notifiable.
- **Organizations across India** have a directive to report cyber incidents and data breaches to the Indian Computer Emergency Response Team (CERT-In) within a mere six-hour deadline.
- **Hong Kong's Critical Infrastructure (CI) security regulation** becomes effective Jan. 1, 2026. It mandates cybersecurity measures and reporting, certain incidents must be reported to the Commissioner's Office within 12 hours.

Organizations must have predefined playbooks, incident response plans, and communication channels to satisfy those reporting timeframes.

RECOMMENDATION:

If it happens, be ready with clear reporting protocols, documented chain of command including legal and PR teams, responsible individuals, and full process workflow to comply with reporting regulations as well as communication with customers and possibly the public. Failure to comply can result in significant fines, reputational damage and legal liability.



Key Steps for Compliance

From minimum security posture to third-party risk and incident reporting, each of the above points are mandated by today's most influential frameworks, standards, and regulations. Align to one or two core frameworks (e.g., NIST CSF 2.0 + ISO 27001) and map sector-specific regulations (PCI-DSS, DORA, HIPAA, etc.) with the corresponding country where the organization operates. Audits should turn into routine control validations and provide executives with consistent risk status backed by industry best practices and compliance.

When looking at what frameworks and regulations your organization can implement to become complaint it is important to take a wholistic approach. Every part of the organization can touch another aspect of the environment. Planning and forethought will play a huge role in assuring your organization's compliance.

Some steps to consider include:

- **Develop a risk management process:** This involves identifying all potential IT risks that could affect your business as well as assessing your vulnerabilities.
- **Analyze and prioritize your risks:** This can be done through developing a risk mitigation strategy and training your staff.
- **Develop an incident response plan:** In this plan, you can consider things like risk transfer while maintaining visibility and insight of your environment.
- **Establish a culture of security:** This can look like involving all relevant stakeholders, picking the right technologies, and never forgetting to document, document, document.

Conclusion

The regulatory landscape is dynamic, and the pace of regulatory change is unlikely to slow down, particularly as governments and regulatory bodies respond to increased cyberattacks. With that in mind, the direction is for organizations to adapt IT and security standards and frameworks to continue to meet regulatory compliance. This helps with the standardization of security best practices which are all about improving security posture beyond the minimum compliance requirements.

In conclusion, regulatory compliance is an ongoing journey that requires continuous effort, adaptation, and collaboration. It is not enough to simply achieve compliance; organizations must strive to maintain and enhance their compliance programs in the face of evolving threats and regulations. Security leaders and IT decision-makers play a crucial role in this process, guiding their organizations toward a compliance strategy that is not only about avoiding penalties but about building a stronger, more cyber resilient organization. By integrating compliance into the fabric of the organization's operations and culture, and by staying informed and agile in the face of change, organizations can navigate the complexities of the regulatory landscape with confidence and success.

READY TO SEE HOW VEEAM CAN HELP YOUR ORGANIZATION?

- Check out this webinar for more tips on strengthening data protection through compliance
- Explore more resources: Analyst reports, customer stories, and technical briefs at veeam.com
- Contact us

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes businesses should control all their data whenever and wherever they need it. Veeam provides data resilience through data backup, data recovery, data portability, data security, and data intelligence. Based in Seattle, Veeam protects over 550,000 customers worldwide who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.