# Security Frameworks

The TechTarget article "Top 12 IT Security Frameworks and Standards Explained" by Paul Kirvan provides an overview of key IT security frameworks and standards, offering guidance on selecting the most appropriate one.

## IT Security Standards, Regulations and Frameworks

- Standards are detailed guidelines outlining specific steps and requirements for implementing security controls.
- Regulations are legally binding directives, such as HIPAA, PCI DSS and GDPR, mandating compliance and often carrying penalties for non-compliance.
- Frameworks are structured sets of best practices and processes designed to help organisations manage and mitigate security risks effectively.

## Importance of Security Frameworks

**Risk Management:** Frameworks provide a structured approach to identifying, assessing and mitigating security risks.

**Compliance:** Frameworks assist in aligning organisational practices with regulatory requirements, facilitating audits and certifications.

**Customisation:** Frameworks can be tailored to address specific industry needs, organisational sizes and threat landscapes.

## Notable IT Security Frameworks and Standards

Kirvan (2021) highlights several prominent frameworks and standards each with specific regional applications and relevance to various sectors:

- **ISO 27000 Series:** A comprehensive set of standards for establishing, implementing and maintaining an Information Security Management System (ISMS).
- **NIST SP 800-53:** Provides a catalogue of security and privacy controls for information systems and organisations.
- **COBIT:** Focuses on governance and management of enterprise IT.
- **CIS Controls**: Offers a prioritised set of actions to protect organisations from cyber threats.
- **HITRUST CSF:** Integrates various standards and regulations, tailored for the healthcare industry.
- **PCI DSS:** Specifies security measures for organisations handling credit card information.
- **GDPR:** Regulates data protection and privacy.
- **HIPAA:** Sets standards for protecting sensitive patient health information.
- **Sarbanes-Oxley Act (SOX):** Mandates financial transparency and accuracy for publicly traded companies.
- **FISMA:** Requires agencies to develop, document and implement information security programs.
- **GLBA:** Protects consumers' personal financial information held by financial institutions.
- **FERPA:** Governs access to educational information and records.

## 1. International Bank

### Applicable Frameworks:

| | |
|---|---|
| ISO/IEC 27001 | For establishing an Information Security Management System (ISMS). |
| NIST Cybersecurity Framework (CSF) | For risk management and resilience. |
| COBIT | For IT governance and aligning IT goals with business. |
| PCI DSS | If handling payment card transactions. |
| GLBA | To comply with data protection requirements in financial services. |
| SOX | For financial reporting compliance. |

### Tests:

- Penetration testing on digital banking systems.
- Regular audits for PCI DSS and ISO 27001 compliance.
- Review of IT governance against COBIT principles.

### Recommendations:

- Implement ISO 27001 to govern security policies across branches.
- Use COBIT to integrate IT risk management into strategic planning.
- Ensure PCI DSS compliance for all payment card systems.
- Maintain rigorous documentation and reporting to meet standards.

## 2. Large Hospital

### Applicable Frameworks:

| | |
|---|---|
| HITRUST CSF | Tailored for healthcare, incorporating HIPAA, ISO, NIST. |
| ISO/IEC 27001 | General security management system. |
| NIST SP 800-53 or CSF | For compliance and broader cyber risk controls. |
| HIPAA | For compliance with United States patient data privacy laws. |

### Tests:

- Security audits on patient record systems and data access controls.
- Regular HIPAA and HITRUST compliance assessments.
- Incident response simulations and tabletop exercises.

### Recommendations:

- Adopt HITRUST CSF for a unified healthcare specific framework.
- Establish policies that enforce access control and encryption.
- Train staff on HIPAA compliance and cybersecurity.
- Use NIST CSF for broader cybersecurity risk assessment and resilience.

### 3. Large Food Manufacturing Factory

#### Applicable Frameworks:

| | |
|---|---|
| ISO/IEC 27001 | General IT and data security. |
| ISO 22000 | Specific to food safety management systems. |
| PCI DSS | If the factory deals with payment processing. |
| NIST CSF | For identifying and reducing cybersecurity risks. |
| COBIT | For IT and operational alignment. |

#### Tests:

- Evaluate operational systems for cyber vulnerabilities.
- Audit Information Technology and Operational Technology segmentation and data flows.
- Conduct supplier risk assessments.

#### Recommendations:

- Implement ISO 27001 to protect intellectual property and operations.
- Integrate ISO 22000 for food safety risk management.
- Use NIST CSF to evaluate and improve cyber hygiene.
- Develop a business continuity plan (BCP) for cyber or supply chain disruptions.

## References

**Kirvan, P.** (2022) *IT security frameworks and standards: Choosing the right one*. TechTarget. Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one (Accessed: 8 April 2025).

## Bibliography

**AuditBoard** (n.d.) *What is the Sarbanes-Oxley (SOX) Act?*. Available at: https://www.auditboard.com/blog/sarbanes-oxley-act/ (Accessed: 8 April 2025).

**Center for Internet Security (CIS)** (n.d.) *CIS Critical Security Controls*. Available at: https://www.cisecurity.org/controls (Accessed: 8 April 2025).

**Compliant FM** (n.d.) *ISO 27001*. Available at: https://compliantfm.com/service/iso-27001/ (Accessed: 8 April 2025).

**Federal Trade Commission (FTC)** (n.d.) *Gramm-Leach-Bliley Act*. Available at: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act (Accessed: 8 April 2025).

**GDPR Info** (n.d.) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/ (Accessed: 8 April 2025).

**HITRUST Alliance** (n.d.) *HITRUST Framework*. Available at: https://hitrustalliance.net/hitrust-framework (Accessed: 8 April 2025).

**ISACA** (n.d.) *COBIT Framework*. Available at: https://www.isaca.org/resources/cobit (Accessed: 8 April 2025).

**National Institute of Standards and Technology (NIST)** (2024) *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5, Update 1)*. Available at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (Accessed: 8 April 2025).

**National Institute of Standards and Technology (NIST)** (n.d.) *Federal Information Security Modernization Act (FISMA)*. Available at: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma (Accessed: 8 April 2025).

**PCI Security Standards Council** (n.d.) *Official PCI Security Standards*. Available at: https://www.pcisecuritystandards.org/ (Accessed: 8 April 2025).

**U.S. Department of Education** (n.d.) *FERPA – Protecting Student Privacy*. Available at: https://studentprivacy.ed.gov/ferpa (Accessed: 8 April 2025).

**U.S. Department of Health & Human Services (HHS)** (n.d.) *HIPAA for Professionals*. Available at: https://www.hhs.gov/hipaa/for-professionals/index.html (Accessed: 8 April 2025).