Integrity360
your security in mind

Which cyber security framework is right for your business?

INCLUDING SEVEN OF THE MOST EFFECTIVE CYBER SECURITY FRAMEWORKS BEING USED TODAY

Integrity360
your **security** in mind

> “There’s no such thing as ‘perfect protection’; continuously assess how much risk is appropriate, and take a systematic approach to implementing a security strategy.”

Sean Rooney,
Cyber Security Strategy Director, Integrity360

Executive summary

Information security requirements have seen substantial change over the last decade, and are set to continue that transformation given the evolving threat landscape, complex regulations and the fast-paced nature of modern business.

Your organisation isn't the only one feeling overwhelmed by all of this, and it's difficult to know if we're doing enough to mitigate the risks. We've accepted a societal norm of, "it's not an if, it's a when," in reference to data breaches. This has led to the vast majority of businesses adopting the newest technologies to combat the latest threats.

However, relying on the technology alone can lull many businesses into a false sense of security. When all it takes is one click or a slight deception from a malicious threat actor to gain access to the network, what then—if anything—can we do to gain some semblance of control?

Cyber security frameworks have become a powerful tool for the organisations that buy into their potential value. Established cyber security frameworks tell you not only how to build the house, but when, where and why you should hammer the nails, too.

In the world of information security, frameworks have been designed to provide a reference for those developing and implementing internal security controls to ensure the business collectively learns from the successes and failures of the cyber security community at large.

These frameworks allow us to take a systematic approach to securing our customers' high-value assets. When paired with intuitive solutions like security information and event management (SIEM) platforms they can give us unparalleled visibility and granular insights into our clients' digital infrastructures, and allow us to take an adaptive approach to protecting sensitive information.

In this guide we'll talk about seven of the most popular cyber security frameworks being used by businesses around the world.

Sean Rooney,
Cyber Security Strategy Director, Integrity360

Why are cyber security frameworks important?

Blueprints for homes and commercial buildings help construction companies ensure they meet a variety of mandates, like energy efficiency or ventilation requirements—that they have all the bases covered. Cyber security frameworks function in a similar way.

Whether it's Sarbanes-Oxley (SOX) for financial institutions, or Payment Card Industry Data Security Standards (PCI DSS) for retailers, each business has regulatory obligations to meet—and they must prove they're meeting them.

By adopting a formal structure, organisations can document exactly what actions they're taking to address compliance, allowing them to spend less time focusing on how to carry out the requirements, and more on critical business functions.

Furthermore, many of the most popular frameworks help to defend against one of the inherent dangers of adopting cyber security technologies: Hackers' attempts evolving quicker than we can detect and respond to them.

Frameworks accomplish this by enabling companies to develop strategies that define the best approach to take when faced with a potential threat on the network. This results in a shift in how cyber security is seen by the organisation: From a requirement viewed as a burden or waste of resources, to an essential function of the business itself.

This line of thought is how organisations must approach cyber security moving forward if they want their initiatives to succeed. In doing so, they protect the company's reputation from repercussions of a data breach, and ensure that the proper response is taken in light of an attacker breaking through the defences.

Every business has regulatory obligations to meet - and they must prove they're meeting them

1 Cyber Essentials

The **Cyber Essentials framework** serves as a fundamental approach to reducing risk regarding digital vulnerabilities that can be found in an organisation's infrastructure. Adopting the strategy can prevent up to 80 percent of potential attacks, according to the National Cyber Security Centre. The framework addresses five components:

DEFAULT CONFIGURATIONS

Can contain passwords to administrator access that are well known among the hacking community. Developing internal configurations and applying system hardening techniques can negate the chance that a run-of-the-mill attempt infiltrates the network.

FIREWALLS AND INTERNET GATEWAYS

Unprotected networks leave organisations vulnerable to common attacks. Ensuring that a firewall and other tools restrict access to pre-approved devices can protect a company from these threats.

USER ACCESS CONTROLS

A lack of effective user access management can lead to compromised administrative accounts. Limit privileges to trusted personnel, and set permissions to minimum for applications and devices.

MALWARE PROTECTION

The number of different methods hackers use to infect systems with malware grows every day. Organisations should ensure any device connected to the internet has the latest virus and malware protection software running on it.

PATCH MANAGEMENT

Meltdown and Spectre showed that any software or hardware can possess vulnerabilities. Develop a strategy that applies patches immediately after they're released.

2 Center for Internet Security (CIS) Top 20 Controls

The **CIS framework** offers 20 total controls that have an excellent track record of helping organisations secure their assets from some of the most challenging threats that have been encountered.

BASIC

- 01 Inventory and Control of Hardware Assets
- 02 Inventory and Control of Software Assets
- 03 Continuous vulnerability management
- 04 Controlled use of administrative privileges
- 05 Secure configuration for hardware and software on mobile devices, laptops, workstations and servers
- 06 Maintenance, monitoring and analysis of audit logs

FOUNDATIONAL

- 07 Email and web browser protecions
- 08 Malware defenses
- 09 Limitation and control of network ports, protocols, and services
- 10 Data recovery capabilities
- 11 Secure configuration for network devices, such as Firewalls, routers and switches
- 12 Boundary defense
- 13 Data protection
- 14 Controlled access based on the need to know
- 15 Wireless access control
- 16 Account monitoring and control

ORGANIZATIONAL

- 17 Implement a security awareness and training program
- 18 Application software security
- 19 Incident response and management
- 20 Penetration tests and red team exercises

CIS Top 6 Controls

Adopting the top six controls has shown to be effective in mitigating the vast majority of potential cyber risks

01 & 02

INVENTORY OF AUTHORISED AND UNAUTHORISED DEVICES AND SOFTWARE

Issue: The bring your own device (BYOD) culture can be problematic for IT staff without an inventory of approved devices and software, which can help defend against ever-evolving malware.

Solution: Create a whitelist of devices/software using MAC addresses, as well as certificate-based Network Access Control (NAC).

03

CONTINUOUS THREAT AND VULNERABILITY ASSESSMENT AND REMEDIATION

Issue: Relying on signature-based detection only eliminates hackers that aren't evolving their efforts. Continuous assessment allows teams to identify new vulnerabilities or ones that were missed, in a bid to strengthen security.

Solution: Conduct regular risk assessments and ensure that a remediation strategy is in place.

04

CONTROLLED USE OF ADMINISTRATOR PRIVILEGES

Issue: Hackers disguised as administrators have a chance of staying in the system undetected much longer than usual, and employees can go rogue without controls in place to monitor administrators.

Solution: Administrator privilege must be reserved for those who actually need it. Consider implementing a Local Administrator Password Solution (LAPS) to keep passwords safe, and regularly review who has access to what.

05

SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE

Issue: Default configurations are easy for average hackers to get into. Once in, the endpoints allow them to move laterally through the network.

Solution: Evaluate the organisation's configuration for systems and applications and develop a gold standard that incorporates hardening techniques.

06

MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

Issue: Added as the sixth control in April 2018 due to the lack of network visibility of corporate cyber security strategies that don't actively gather and evaluate digital activity.

Solution: Security information and event management (SIEM) software should be used to continuously monitor and assess vulnerable endpoints and movement on the network.

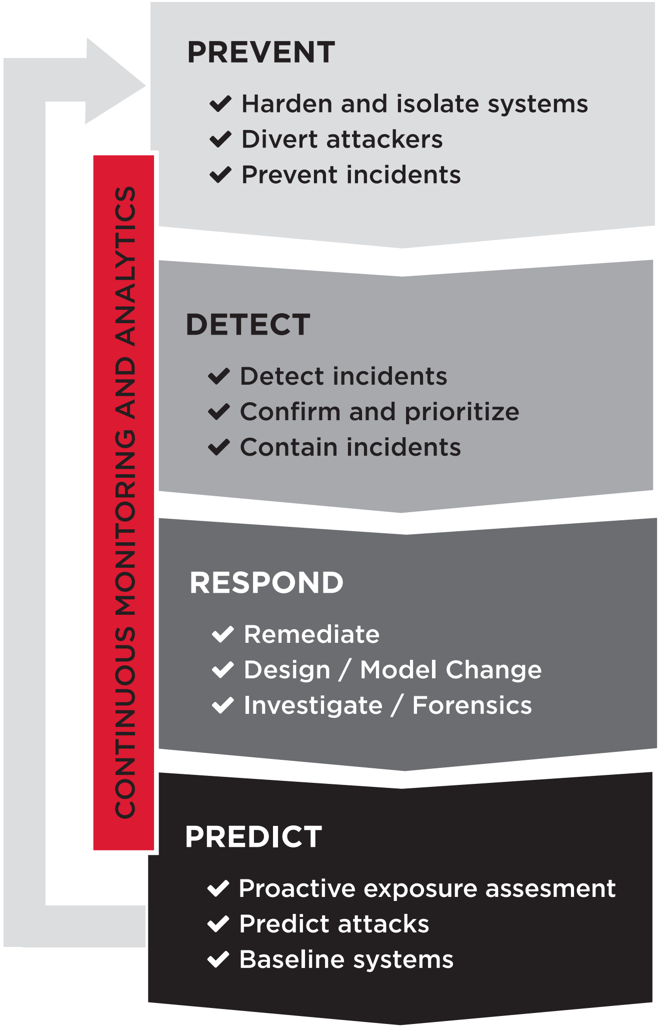
3 Gartner's adaptive security architecture

Companies need to learn how to crawl before they can walk. **The Gartner adaptive security architecture** provides a foundation as to how a business should invest in technological assets, as well as a top-level view of how to structure its general cyber security strategy.

It runs on the principle that too many businesses are taking an approach that puts them in a reactive position; they're left waiting for an attack to take place, rather than a proactive strategy that continuously assumes they're under attack. The latter can lead to consistent evaluation of their posture, which ensures defence mechanisms stay modern.

This cycle—which starts with prevent and ends at predict—represents the 12 critical capabilities that compose a modern cyber security strategy. Of course, it also relies on IT personnel having access to platforms that support functionality like investigations led by digital forensics, or proactive exposure assessments.

The adaptive security architecture



CONTINUOUS MONITORING AND ANALYTICS

PREVENT

- ✓ Harden and isolate systems
- ✓ Divert attackers
- ✓ Prevent incidents

DETECT

- ✓ Detect incidents
- ✓ Confirm and prioritize
- ✓ Contain incidents

RESPOND

- ✓ Remediate
- ✓ Design / Model Change
- ✓ Investigate / Forensics

PREDICT

- ✓ Proactive exposure assesment
- ✓ Predict attacks
- ✓ Baseline systems

NEW SAMPLECLASS(11, 44);
SAMPLECLASS SC2;
MY LOCAL CONSTANT = {0}", MY
ABSTRACT LANGUAGE
CHARSET=CHARSET.UNICODE)]
STRING F, INT TYPE);
ENTER YOUR MESSAGE: ");
CONSOLE.READLINE();
MYSTRING, "MY MESSAGE TEXT", 0);

4 NIST cyber security framework

Known as an agile approach to cyber security, the NIST framework is popular across the world. It's a cost-efficient methodology of building a strategy that's easy for the entire company to adopt.

The NIST cyber security framework is a three-part strategy. The first represents five functions, which contain 22 categories:

Identify: Organisations should have a goal of managing digital assets to deter risk.

Protect: Companies should adopt the appropriate processes and measures to defend against a cyberattack, and remediate network threats.

Detect: Businesses need to quickly respond to threat actors to mitigate their impact.

Respond: Organisations should have a strategy in place to contain cyber threats.

Recover: Companies need to be able to restore operations after an attack.

Unique to NIST are the four tiers of maturity that an organisation can align itself with. These serve as a means of self-evaluating how much—or little—of the framework a company has adopted. These are defined as:

Partial: Organisation has informal risk management processes, limited awareness as to the risk that a lack of cyber security presents, narrow or zero visibility into cyber security supply chain and doesn't search for or share information related to cyber-attacks. I

Risk-informed: Organisation has a formal strategy approved but it isn't implemented, understands the risks presented but cannot resolve them, may read about industry-specific threats but won't share the information. II

Repeatable: Organisation's cyber security policy is adhered to by the entire company, workforce has the individual skill sets to spot rudimentary hacking attempts like phishing, IT departments continuously monitors assets and the company actively examines new intel and shares it within industry. III

Adaptive: Organisation consistently looks to improve its cyber security policy and defensive measures, procedures reflect the high level of importance that cyber risk plays in the eyes of board of directors, proactively searches for new information on threats and shares with industry, leverages real-time data to evaluate safety of assets. IV

NIST CYBER SECURITY FRAMEWORK

The NIST cyber security framework core consists of five functions that contain 22 categories.

1. IDENTIFY

- ✓ Asset management
- ✓ Business environment
- ✓ Governance
- ✓ Risk assessment
- ✓ Risk management strategy

2. PROTECT

- ✓ Awareness control
- ✓ Awareness and training
- ✓ Data security
- ✓ Info protection and procedures
- ✓ Maintenance
- ✓ Protective technology

3. DETECT

- ✓ Anomalies and events
- ✓ Security continuous monitoring
- ✓ Dectection process

4. RESPOND

- ✓ Response planning
- ✓ Communications
- ✓ Analysis
- ✓ Mitigation
- ✓ Improvements

5. RECOVER

- ✓ Recovery planning
- ✓ Improvements
- ✓ Communications

5 ISO 27001

ISO 27001 is a standard for managing risk in relation to the data and high-value assets stored in your organisation. It's part of the **ISO 27000 family of standards** that are designed to keep your business and its digital infrastructure secure.

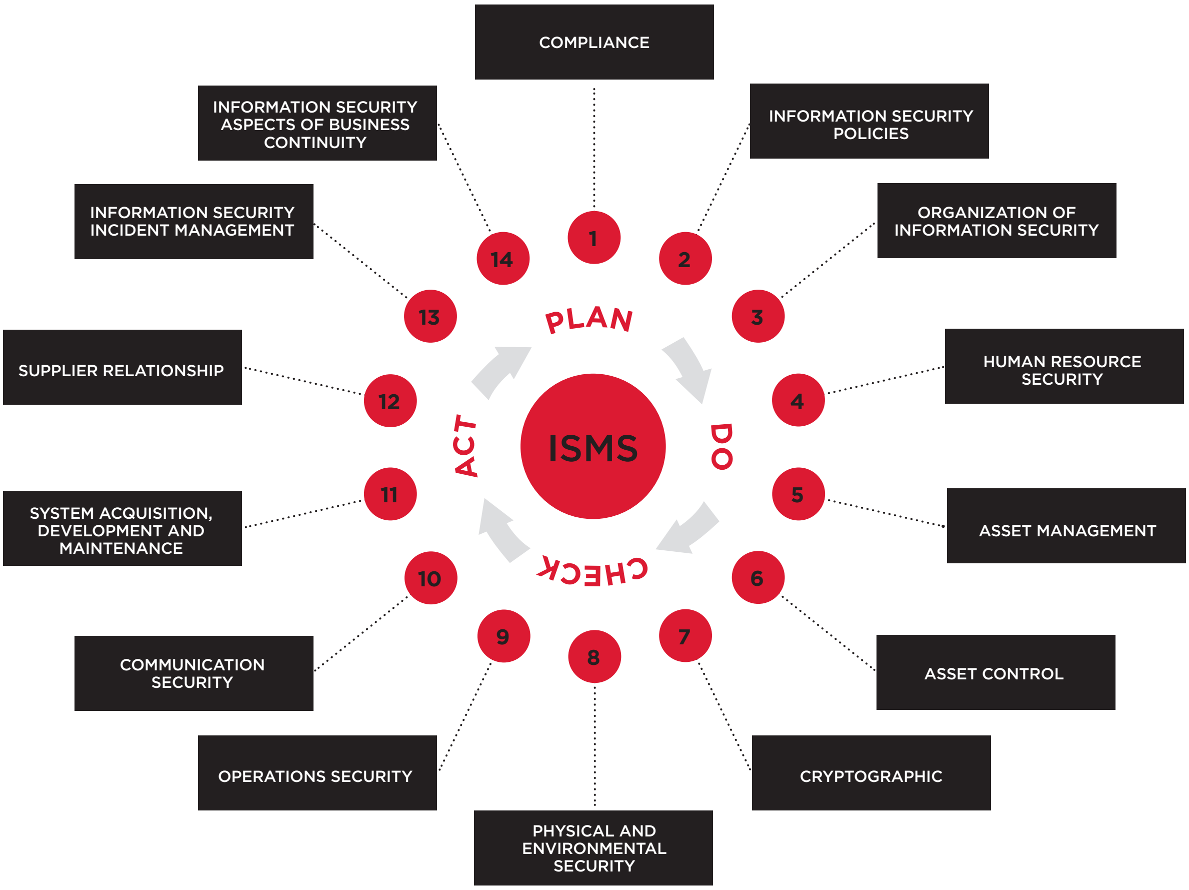
Accredited by an independent certification body (the International Organization for Standardization), the most current version is ISO 27001 (2013). It provides a set of standardised requirements for building and maintaining an Information Security Management System (ISMS).

The standard itself is composed of several 'shall' statements, which companies must comply with. These ensure that:

- ✓ The business objectives are clearly understood.
- ✓ All stakeholders are identified.
- ✓ An appropriate information security governance structure is developed.
- ✓ An effective approach to risk management is established and adopted.
- ✓ A process of continual improvement and monitoring is in place.

ISO 27001

Global standard on information security management systems (ISMS)


COMPLIANCE
INFORMATION SECURITY POLICIES
ORGANIZATION OF INFORMATION SECURITY
HUMAN RESOURCE SECURITY
ASSET MANAGEMENT
ASSET CONTROL
CRYPTOGRAPHIC
PHYSICAL AND ENVIRONMENTAL SECURITY
OPERATIONS SECURITY
COMMUNICATION SECURITY
SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE
SUPPLIER RELATIONSHIP
INFORMATION SECURITY INCIDENT MANAGEMENT
INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY
1
2
3
4
5
6
7
8
9
10
11
12
13
14
PLAN
DO
CHECK
ACT
ISMS

When the risk assessment is carried out, organisations can select applicable controls from the 114 options listed in Annex A, then design and implement security controls around them. These controls are documented in the statement of applicability and from the basis of the audit.

The Annex A controls sections are broken down into the following domains:

- ✓ **A.5** - Information security policies
- ✓ **A.6** - Organization of information security
- ✓ **A.7** - Human resources security
- ✓ **A.8** - Assets
- ✓ **A.9** - Access control
- ✓ **A.10** - Cryptography
- ✓ **A.11** - Physical and environmental security
- ✓ **A.12** - Operational security
- ✓ **A.13** - Communications security
- ✓ **A.14** - System acquisition, development and maintenance
- ✓ **A.15** - Supplier relationships
- ✓ **A.16** - Information security incident management
- ✓ **A.17** - Information security aspects of business continuity management
- ✓ **A.18** – Compliance

As ISO 27001 is an internationally recognised standard, it's an excellent choice for organisations that need to show their clients that they are taking information security seriously. Its strength lies in its ability to define the structure of the ISMS, and how information security should be managed.

The potential downside of ISO 27001 is that it's not prescriptive in terms of specific technical controls that are needed. A certain level of knowledge of the threat landscape, and how to perform a comprehensive risk assessment, is needed to allow for the appropriate design of controls.

6 NIST Special Publication 800-53

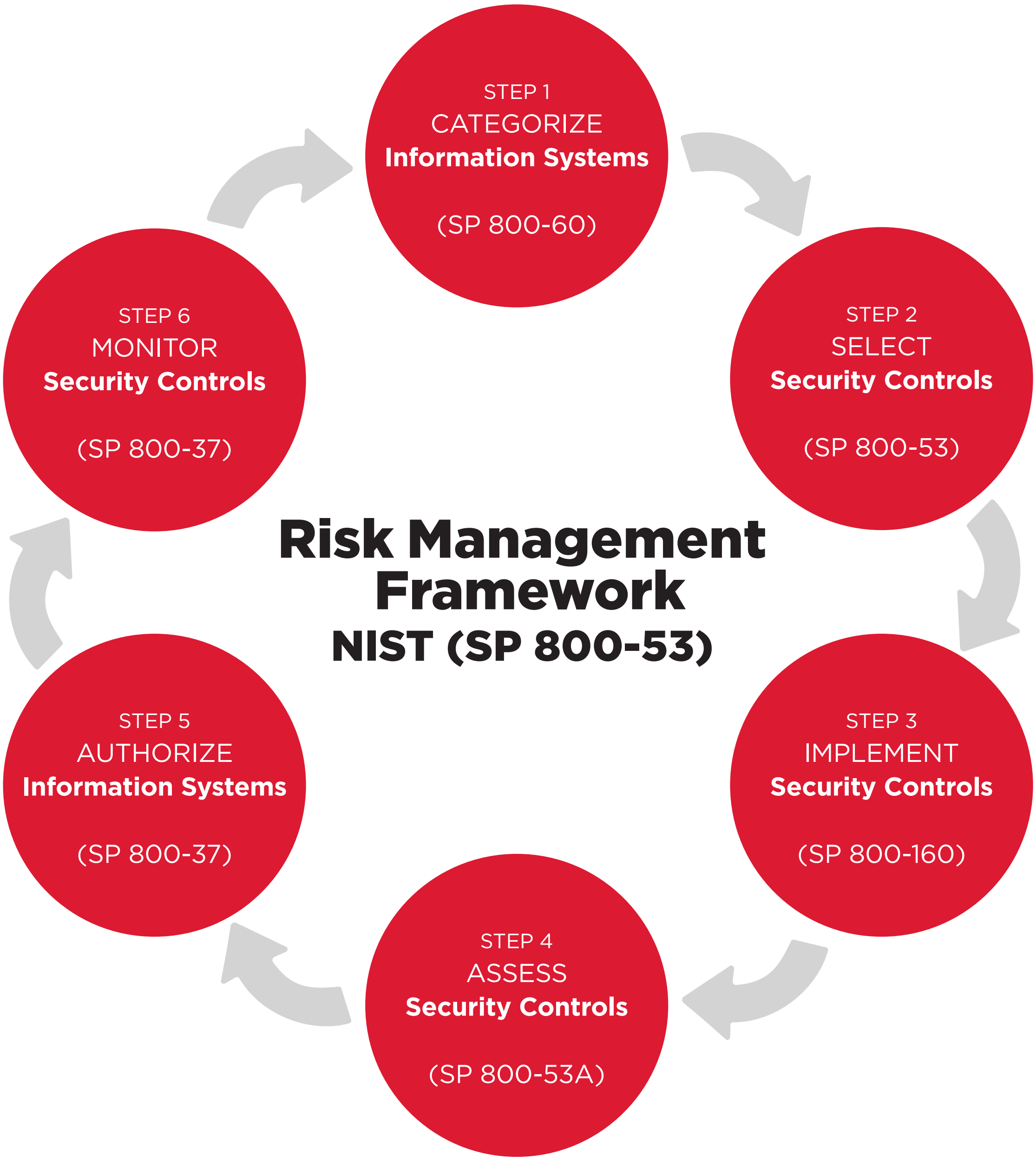
NIST 800-53 is a special publication by NIST that recommends security controls for federal information systems in the US and private organisations. It documents security controls for all federal information systems—except those designed for national security—and outlines the requirements of the Federal Information Processing Standard (FIPS).

NIST 800-53 is a comprehensive framework with a large array of controls and enhancements broken down into low-, medium- and high-impact categories.

NIST 800-53's controls are split into three classes and 18 families

The controls are broken into three classes and split into 18 different families. These are:

- ✓ Access Control
- ✓ Audit and Accountability
- ✓ Awareness and Training
- ✓ Configuration Management
- ✓ Contingency Planning
- ✓ Identification and Authentication
- ✓ Incident Response
- ✓ Maintenance
- ✓ Media Protection
- ✓ Personnel Security
- ✓ Physical and Environmental Protection
- ✓ Planning
- ✓ Program Management
- ✓ Risk Assessment
- ✓ Security Assessment and Authorization
- ✓ System and Communications Protection
- ✓ System and Information Integrity
- ✓ System and Services Acquisition 'critical' or 'high-risk' and required immediate remediation.



Risk Management Framework

NIST (SP 800-53)

STEP 1
CATEGORIZE
Information Systems
(SP 800-60)

STEP 2
SELECT
Security Controls
(SP 800-53)

STEP 3
IMPLEMENT
Security Controls
(SP 800-160)

STEP 4
ASSESS
Security Controls
(SP 800-53A)

STEP 5
AUTHORIZE
Information Systems
(SP 800-37)

STEP 6
MONITOR
Security Controls
(SP 800-37)

7 Internet Security Forum Standard (ISF)

The **ISF's Standard of Good Practice for Information Security 2016** is a comprehensive guide that supports companies as they combat cyber criminals in a quickly evolving environment.

Its main goals provide a foundation for businesses to:

- ✓ Understand and meet regulations.
- ✓ Leverage threat and vulnerability assessments to continue to adapt cyber security strategy in response to emerging risks.
- ✓ Develop organisational agility to meet the resource demand that new threats require.

To achieve this, the Standard provides the following enablers:

Awareness: Instead of creating a cyber security framework from scratch, the ISF provides up-to-date information on risk and vulnerabilities catered to every target audience included in the organisation.

Resilience: The framework includes a guide to prepare the company for an attack, which covers areas like crisis management and business continuity.

Risk assessment: Companies are provided a set of controls that help to refine their threat and vulnerability assessment.

Supply chain management: Businesses are given a solution to align their supply chain risk management processes with ISO/IEC 27036-3:2013.

Compliance: Organisations are equipped with a tool that simplifies compliance to ISO/IEC 27001:2013 standards, as well as industry-specific regulations.

Policies, standards and procedures: Standard is adopted directly as a baseline for internal cyber security policies and procedures.

Security arrangements: Framework serves as the latest reference to state-of-the-art security products that protect businesses from evolving risks.

Information security assessment: The ISF benchmark provides a high-level assessment of the information security controls in place.

Industry-specific regulations

A major benefit in adopting a cyber security framework is that it helps organisations comply with industry-specific and regulatory mandates.

Popular regulations include:

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) states that appropriate technical and organisational controls must be in place for an organisation to fulfil their data protection requirements.

The particular measures are not specified, however, EU Data Protection Supervisor Giovanni Buttarelli said in early 2017 that certification schemes, "could bring great benefits," in helping organisations to navigate the GDPR.

This is one of the inherent benefits of ISO 27001—it allows you to take a risk-based approach to the protection of personal information, and incorporate those data protection requirements and principles into your ISMS, ensuring that you are taking appropriate technical and organisational measures.

Payment Card Industry Data Security Standards (PCI DSS): Organisations that facilitate credit card payments must comply with PCI DSS requirements. These include:

- ✓ Audit or vulnerability assessment that identifies gaps in cyber security coverage.
- ✓ Controls in place that relate to monitoring data processing.

Frameworks like the ISO 27001 or NIST apply the self-evaluation necessary to identify exploits and prove that they're being actively considered regarding the overall cyber security strategy. It's recommended that companies blend their frameworks—the one provided by PCI DSS and others—to develop a comprehensive approach, rather than separate them.

Sarbanes-Oxley Act (SOX): Sarbanes-Oxley does not specifically call for information security controls in sections 302 and 404, but their importance in meeting compliance is implied considering the technological advancement of modern financial and accounting software.

Any process-based framework, such as NIST 800-53, ISO 27001 or Control Objectives for Information and Related Technology (COBIT), can serve a company well in this capacity. They offer organisations the ability to apply a certified methodology as to how members of the organisation should handle sensitive data. Furthermore, they provide a system of self-evaluation, and proof to auditors that the business is doing everything it can to meet SOX objectives.

Cyber security frameworks help organisations comply with industry-specific mandates.

Next Steps

Adopting a cyber security framework isn't the easiest task for an organisation to accomplish. But, those that do find their high-value assets and sensitive client data to be exceptionally well protected. Integrity360 experts are able to provide a wide breadth of services geared to help companies identify their vulnerabilities, gaps in cyber security framework and work closely with them to implement the relevant framework.

Contact Integrity360 today to learn more about our cyber security framework assessment and next-gen SIEM services.

Please email info@integrity360.com or visit integrity360.com for more information.

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 1 293 4027

LONDON OFFICE
90 Long Acre,
Covent Garden, London, WC2E 9RZ
+44 203 397 3414

BIRMINGHAM OFFICE
TS2 Pinewood Business Park,
Coleshill Road, Birmingham, B37 7HG
+44 203 397 3414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1 212 461 3286

Integrity360

your **security** in mind