FLEXENTIAL®

SOLUTION OVERVIEW: ISO 27001, NIST SP 800-53 & NIST SP 800-30

Compliance with Confidence for ISO and NIST

Architecture & Transformation

Optimized Clouds

DevOps

Cybersecurity

› Compliance

Disaster Recovery

PROFESSIONAL SERVICES

ISO and NIST Overview

Managing security, privacy and risk to rigorous and recognized standards improves an organization's security posture and proves to stakeholders that safeguarding information is taken seriously. Compliance with validated frameworks and standards requires discipline, effort and expertise. Flexential Professional Services has extensive compliance expertise and effective assessment methodologies to maximize compliance and minimize organizational risk.

Cybercriminals continually reinvent attack methods to exploit vulnerabilities, so the issue to consider when evaluating vulnerabilities is finding them before a bad actor does. Organizations must also consider how many gaps they have, how risky they are, how to remediate them and most importantly, which remediations to prioritize. Finally, while it is far more preferable to prevent security breaches, it's critical to think about responses: threat detection, alerting, response and containment. Together, these multi-layered threat prevention and response activities create defense in depth.

For effectively structuring these activities, organizations use well-established and respected security frameworks. Adopting a high-quality framework not only improves security posture; it proves to customers and prospects that security is a serious priority.

Fortunately, there are robust, documented best practices and guidance for information security management systems (ISMS), security, privacy and risk: ISO 27001, NIST SP 800-53 and NIST SP 800-30. While ISO 27001 offers actual certification and NIST SP 800-53 does not, both frameworks support building effective defenses that mitigate security risks and build trust with external stakeholders. While not a specific framework, NIST SP 800-30 is a Special Publication that provides guidance for conducting risk assessments.

ISO 27001, NIST SP 800-53 and NIST SP 800-30 are applicable to any organization, across all industries, for addressing security and risk mitigation. The International Organization for Standardization's (ISO) purpose is to create international standards for best practices applicable to a wide variety of organizations. The ISO 27001:2013 standard specifically addresses ISMS. The National Institute for Standards and Technology (NIST) creates standards for the federal government and organizations that wish to do business with the federal government. The entire set of NIST standards have broad adoption with both the federal supply chain and non-supply chain organizations looking to improve risk and security postures.

> Frameworks for compliance and cybersecurity provide a common language which can be used at all levels of an organization to promote more secure and efficient business practices while empowering the enterprise to meet its legal responsibilities to consumers, industry governing bodies, and regulatory authorities.[1]

Organizations that fall short in complying with one of these frameworks leave themselves open to attacks that typically result in reputation damage, lost productivity and missed business revenue. By adhering to ISO 27001 or NIST SP 800-53, an organization demonstrates to the outside world that it has rigorous, standards-based security practices in place to actively mitigate risk.

Whether an organization is just beginning to use or already using an ISO or NIST framework, an external partner can help assess and efficiently navigate a compliance journey.

Summary of ISO and NIST Standards for Security, Privacy and Risk

	ISO 27001	NIST SP 800-53	NIST SP 800-30
Basic Summary	Provides requirements for establishing, implementing, maintaining and continually improving ISMS. Comprised of 114 controls across 14 control sets that must be proven and documented for certification.	A comprehensive and flexible catalog of security and privacy controls to meet current and future protection needs based on changing threats, vulnerabilities, requirements and technologies.[2] Comprised of 1189 security and privacy controls across 20 control families.	Provides detailed guidance on preparing, conducting and maintaining a risk assessment, including proper communication and sharing of the assessment results and risk-related information.
Application	Internationally recognized ISMS standard for organizations of all sizes and industries.	U.S. Department of Commerce framework with requirements for U.S. Federal government systems and organizations; is also widely used across industries.	U.S. Department of Commerce guide for conducting risk assessments. Widely used across industries.
Certification	Exacting, highly detailed certification requirements	No formal certification	No formal certification
Implementation	Onerous preparation and costly certification assessment, but standards can be followed without official certification.	Framework implementation can be prioritized and tailored to time, budget limitations and business objectives.	Risk assessment can be done in-house or by outside professionals.

ISO and NIST Challenges

Factors that prevent organizations from properly adopting and adhering to these frameworks:

- Unknown or unaddressed compliance gaps
- Lack of risk awareness & management
- Shortage of staff experienced with compliance standards
- Absence of a cohesive compliance strategy
- Insufficient upper management support
- Inadequate funding

Flexential's Approach

Hallmarks of the Flexential Professional Services compliance approach include:

- Risk-based
- Consultative
- Tailored engagements
- Detailed, actionable and prioritized guidance
- Highly certified security and compliance experts

Flexential Professional Services for Security, Privacy and Risk Compliance

Assessments and gap analysis can reveal which existing practices are effective and which areas need improvement to comply with ISO 27001 or NIST SP 800-53 frameworks. Flexential's expertise in recommendations, guidance, remediation and program development provides a risk-based approach and prioritized roadmap to improve security and reduce risk. Flexential tailors all services to customer-specific considerations to maximize return on investments of time and budget. All services and recommended remediation actions are based on risk mitigation best practices, regardless of the chosen compliance framework.

Flexential Professional Services for ISO and NIST

ISO	NIST
• ISO 27001 Gap Analysis • ISO 27001 ISMS Maturity Assessment	• NIST SP 800-53 Gap Analysis • NIST SP 800-53 Security Assessment • NIST SP 800-30 Risk Assessment

Effective Assessments & Expert Guidance

Customers receive prioritized, detailed, actionable guidance on what to remediate and how.	Gain practical information to implement best practices and mitigate risks.
CISSP-certified professional assessment team has security experience across multiple industries.	Know exactly which standards to follow and how to meet them.
Flexential tailors services to each customer engagement.	Maximize value and ROI with services adapted to customer-specific needs.
Broad compliance expertise and services that can fulfill multiple frameworks and requirements.	Approach compliance holistically.

Organizations that adopt and comply with a recognized security framework improve their security posture and communicate to stakeholders their prioritization of security, privacy and risk. However, lack of time, expertise or budget often hampers organizations from thoroughly assessing their current posture and efforts—and then systematically improving and maintaining them to standards. Failing to achieve or maintain compliance with an established information security management framework puts an organization at risk and communicates to clients and prospects that security is not a serious priority.

Flexential Professional Services can tailor a solution to fit customer-specific compliance needs: whether an organization needs to meet customer demands for security, build stakeholder trust, strengthen the organization's brand image or wants to identify and remediate risks that could cause the most harm. Flexential's highly certified and experienced experts help organizations achieve NIST and ISO compliance faster and more confidently, while documentation and knowledge transfer empower internal teams to maintain compliance in the future.

Flexential Professional Services Security, Privacy and Risk Certifications

Certified Information Systems Security Professional

Certified Information Systems Auditor

Certified Information Security Manager

Certified in Risk and Information Systems Control

Certified in the Governance of Enterprise IT

Certified Data Privacy Solutions Engineer

Payment Card Industry Qualified Security Assessor

HealthCare Information Security and Privacy Practitioner

Cybersecurity Maturity Model Certification AB Registered Provider Organization

Cybersecurity Maturity Model Certification AB Registered Practitioner

Offensive Security Certified Professional

Offensive Security Certified Expert

Offensive Security Wireless Professional

EC-Council Certified Incident Handler

Encase Certified Examiner

Systems Security Certified Practitioner

[1] Cybersecurity Compliance Frameworks." FinJan Cybersecurity Blog, FinJan, 6 Aug. 2018, blog.finjan.com/cybersecurity-compliance-frameworks/

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

ABOUT FLEXENTIAL

Flexential empowers the IT journey of the nation's most complex businesses by offering flexible and tailored hybrid IT solutions comprised of colocation, cloud, connectivity, data protection, managed, and professional services. The company builds on a platform of three million square feet of data center space in 20 highly connected markets, and on the FlexAnywhereTM 100GB private backbone to meet the most stringent challenges in security, compliance, and resiliency. See how Flexential goes beyond the four walls of the data center to empower IT through an interactive map found on www.flexential.com.