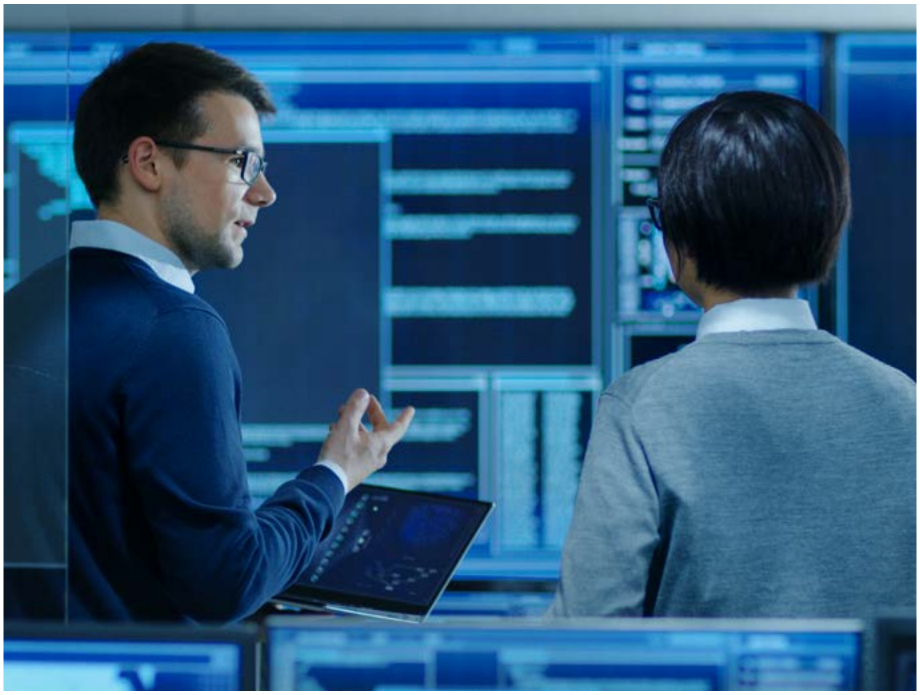
BDO KNOWS:

CYBERSECURITY



RISK MANAGEMENT FRAMEWORKS COMPARISON

FRAMEWORK OVERVIEW

Organizations, no matter how large or small or how long they have been in business, have technology related tasks that require some level of effort to be put forth. The efforts can vary depending on the services the organization provides, the data they have access to, or the intellectual property they maintain. The organization may also have to demonstrate how they are securing their environment, what business controls are in place, and if they are interacting with other companies, including healthcare organizations, financial institutions, or government organizations. There are multiple cybersecurity risk management frameworks that can help an organization evaluate the robustness of the security and controls they have implemented. The current cybersecurity risk management frameworks tend to have a combination of security and compliance requirements, in an effort to enhance the organization's technology environment. The numerous cybersecurity risk management frameworks are managed by multiple, independent groups.

This is an excerpt from *Cybersecurity in the Digital Age*. To learn more about risk management frameworks, please contact:

GREG SCHU
Partner, Cybersecurity
Advisory Services
612-367-3045
gschu@bdo.com

GREGG GARRETT
Head of U.S. and International
Cybersecurity Advisory Services
703-893-0600
ggarrett@bdo.com

A snapshot of the representative groups includes:

AICPA SOC
AICPA Service Organization Control Reports
aicpa.org/soc
Formerly SAS 70 Reports
ISO
IEC
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
PCI
Security Standards Council
HITRUST
CSF Certified
HIPAA
Health Insurance Portability and Accountability Act

Compliance focused requirements tend to focus on protecting specific data. Common frameworks are:

- GDPR (General Data Protection Regulation)
- GLBA (Gramm-Leach Bliley Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- HITRUST (The Health Information Trust Alliance)
- SOX (Sarbanes-Oxley Act)
- PCI DSS (Payment Card Industry Data Security Standard)
- SOC (Systems and Organization Controls)
- FISMA (Federal Information Security Management Act)

Security focused requirements focus on an organization's environment, such as:

- NIST (National Institute of Standards and Technology)
- ISO (International Standards Organization)

Another way to analyze the requirements is to drop them in to the buckets they are commonly viewed as:

Regulatory	Contractually Enforced	Voluntary
GDPR	PCI DSS	NIST
GLBA	SSAE18 (SOC1)	ISO
FISMA	SOC 2	
HIPAA	HITRUST	
SOX		

HOW TO USE THE GUIDANCE

When assessing the above stated cybersecurity risk management frameworks there are a few terms to take in to consideration. The following are some of the key definitions to apply to the organizational assessment structures.

- **Framework:** the basic structure of something; a supporting structure; a structural frame.
- **Oversight**: A structure through which an organization directs, manages and reports its security management activities. It defines roles and responsibilities, decision, risk governance, and reporting lines.
- **People:** A strong security culture helps to encourage strategic decisions that are in the long-term best interest of the organization, its shareholders, and employees.
- **Processes:** The activities in place that allow an organization to identify, assess and quantify known and emerging security risks. It encompasses processes, tools, and systems.
- **Technology:** It includes development tools, software, databases, technology architecture, and systems that support risk management.

To expand on terminology and definitions, further details about requirements and standards have been gathered to help evaluate which standard may be applicable to an organization.

Standard/Framework	Description
National Institute of Standards and Technology (NIST)	NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems. NIST works closely with federal agencies to improve their understanding and implementation of FISMA to protect their information and information systems, and publishes standards and guidelines which provide the foundation for strong information security programs at agencies. NIST performs its statutory responsibilities through the Computer Security Division of the Information Technology Laboratory. NIST is in the U.S. Department of Commerce NIST guidance selected by organizations include (but are not limited to): ▶ 800-30 (Risk management) ▶ 800-53 (Recommended security controls for Federal Information Systems and Organizations) ▶ 800-57 (Cryptographic key changes) ▶ 800-66 (Intro guide for implementing HIPAA security) ▶ 800-115 (Penetration methodology) ▶ 800-171 (Cybersecurity standard or formally - Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organization)
Federal Information Security Management Act of 2002 (FISMA)	FISMA is a United States federal law passed in 2002 that made it a requirement for federal agencies to develop, document, and implement an information security and protection program. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, was developed in support of FISMA. NIST SP 800-53 is the primary source of recommended security controls for Federal agencies. It describes several controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken due to audit failure.
ISO 2700x	ISO is an international standard, with worldwide recognition, which lays down the requirements for the establishment of an information security management system. It applies to any type of organization, and their implementation and certification is optional, so it is not mandatory for a company. ISO/IEC27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). ISO is governed by the International Organization for Standardization

Standard/Framework	Description
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	HIPAA is U.S. legislation that provides data privacy and security provisions for safeguarding medical information. HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the **HIPAA Privacy Rule and the HIPAA Security Rule**.
System and Organization Controls (SOC)	SOC 1 is a report on controls at a service organization relevant to a user entity's internal control over financial reporting. SOC 2 is a report on the Trust Services Principles. The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. SOC assessments are governed by the **American Institute of CPAs (AICPA)**.
Payment Card Industry Data Security Standard (PCI DSS)	PCI-DSS is an information security standard for organizations that process, store, transmit or could impact the security of the cardholder data environment. The PCI DSS pertains to branded credit and debit cards for the following card brands: Visa, MasterCard, Discover, American Express and JCB. The **Payment Card Industry Security Standards Council (PCI SSC)** manages and maintains the PCI DSS.
Gramm-Leach-Bliley Act (GLB Act or GLBA)	GLBA is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. GLBA requires financial institutions that offer consumers financial products or services like loans, financial or investment advice, or insurance, to explain their information-sharing practices to their customers and to safeguard sensitive data. GLBA is governed by the **Federal Trade Commission (FTC)**.
Sarbanes-Oxley Act (SOX) of 2002	SOX is a U.S. federal law that set new or expanded requirements for all U.S. **public company** boards, management and public accounting firms. There are a number of provisions of the Act that also apply to privately held companies; for example, the willful destruction of evidence to impede a Federal investigation. The bill, which contains eleven sections, was enacted as a reaction to a number of major **corporate and accounting scandals**, including Enron and WorldCom. As a result of SOX, top management must individually certify the **accuracy of financial information**.

Standard/Framework	Description
General Data Protection Regulation (GDPR)	GDPR is a regulation in European Union (EU) law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the **1995 Data Protection Directive (Directive 95/46/EC)**. GDPR was adopted on 27 April 2016 and becomes enforceable 25 May 2018; after a two-year transition period. Unlike a directive, it does not require national governments to pass any enabling legislation and so it is directly binding and applicable.

CYBERSECURITY RISK MANAGEMENT FRAMEWORKS — COMPARISON

To expand on the information provided above regarding UCF and CCF, a comparison has been mapped out to indicate possible areas of overlap to the five NIST cybersecurity – Identify; Protect; Detect; Respond; and Recovery. When reading through the cybersecurity focus areas, the cross-over of categories, sub-categories and corresponding reference information clarify the controls and requirements that are common across multiple risk management frameworks.

Identity

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	▶ ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ▶ NIST SP 800-53 Rev. 4 CM-8 ▶ PCI DSS v3.2 2.4, 9.9, 1.1.1
		ID.AM-2: Software platforms and applications within the organization are inventoried	▶ ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ▶ NIST SP 800-53 Rev. 4 CM-8 ▶ PCI DSS v3.2 2.4
		ID.AM-3: Organizational communication and data flows are mapped	▶ ISO/IEC 27001:2013 A.13.2.1 ▶ NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 ▶ PCI DSS v3.2 1.1.2, 1.1.3
		ID.AM-1: Physical devices and systems within the organization are inventoried	▶ ISO/IEC 27001:2013 A.11.2.6 ▶ NIST SP 800-53 Rev. 4 AC-20, SA-9 ▶ PCI DSS v3.2 8.1.5

Protect

Function	Category	Subcategory	Informative References
PROTECT (PR)	Identity Management and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	▶ ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 ▶ NIST SP 800-53 Rev. 4 AC-2, IA Family ▶ PCI DSS v3.2 8.1, 8.2, 12.3
		PR.AC-2: Physical access to assets is managed and protected	▶ ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, ▶ A.11.1.6, A.11.2.3 ▶ NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, ▶ PE-9 ▶ PCI DSS v3.2 9.1, 9.2, 9.3, 9.4, 9.5, 9.9, 9.10
		PR.AC-3: Remote access is managed	▶ ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 ▶ NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 ▶ PCI DSS v3.2 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10

Detect

Function	Category	Subcategory	Informative References
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	▶ NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	▶ ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 ▶ NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 ▶ PCI DSS v3.2 10.6.1, 11.4, 12.5.2
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	▶ NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, ▶ SI-4 ▶ PCI DSS v3.2 10.1, 12.10.5

Respond

Function	Category	Subcategory	Informative References
RESPOND (RS)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	▶ ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 ▶ NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 ▶ PCI DSS v3.2 12.10
		RS.CO-2: Events are reported consistent with established criteria	▶ ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 ▶ NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 ▶ PCI DSS v3.2 12.10
		RS.CO-3: Information is shared consistent with response plans	▶ ISO/IEC 27001:2013 A.16.1.2 ▶ NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, ▶ PE-6, RA-5, SI-4 ▶ PCI DSS v3.2 12.10

Recovery

Function	Category	Subcategory	Informative References
RECOVERY (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	▶ ISO/IEC 27001:2013 A.16.1.5 ▶ NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 ▶ PCI DSS v3.2 12.10.6
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 PCI DSS v3.2 12.10.6

This concludes the overview of cybersecurity risk management frameworks that are used by organizations to comply with regulatory requirements and/or to enhance the day-to-day control and security framework applicable to the technology platforms implemented.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 80,000 people working out of 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.