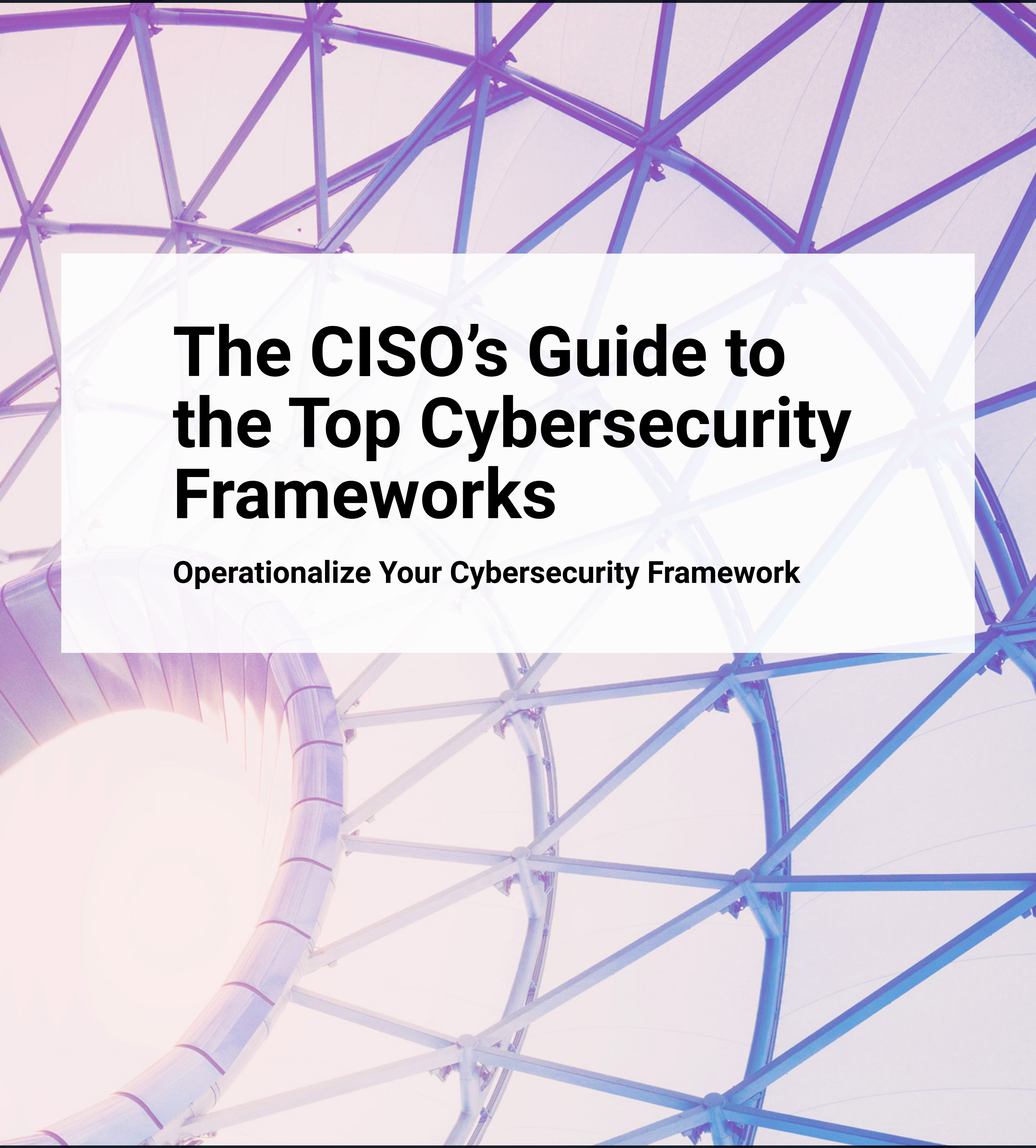


The CISO’s Guide to the Top Cybersecurity Frameworks

Operationalize Your Cybersecurity Framework

Notice

This publication is provided for information purposes only. At the time of publication, all of the information within this publication is as accurate and current as could be determined. Any additional data since publication will not be added or updated to this report. AttackIQ, Inc. is not responsible for errors or omissions in the context of this report or for damages arising from the use of this report under any circumstances. Finally, please note that this publication may be updated or changed without notice.

Table of Contents

Executive Summary

This report will overview six of the most important cybersecurity and information technology frameworks used by enterprises and governments today. The frameworks covered include ISO 2700, CIS Controls®, NIST CSF, ISACA®'s COBIT® 2019, the Lockheed Martin Cyber Kill Chain®, and MITRE ATT&CK®. Appendix A in this document lists other important frameworks.

Over the past few years, increasingly successful cyber attacks have driven frameworks into the spotlight. The structure and best practices brought by these frameworks help organizations plan, execute, and respond faster and better to these threats, allowing rapid return to normal business operations.

Tenable® Inc. did a survey and report on frameworks in 2016 in which 84 percent of the 338 enterprises interviewed leveraged a security framework[1]. At the time of the survey, more than 44 percent used more than one security framework. NIST CSF, CIS-CSC, and ISO 27001 were prominent across the surveyed institutions. Not surprisingly, banks and financial institutions had the highest framework adoption rate at that time.

In 2020, the rate of framework adoption has greatly accelerated. Data suggests that in large global enterprises, market share for CIS-CSC, ISO 27001, and ISACA's COBIT (5 & 2019) is well over 30 percent each. Most have multiple frameworks in use. These frameworks are all popular, along with NIST CSF and the expanded family of NIST cybersecurity standards.

MITRE ATT&CK has also arrived on the scene and is going through rapid adoption due to its unique attributes and special orientation. MITRE ATT&CK presents the best way to think like an attacker and understand and anticipate the tactics, techniques, and procedures they will use. MITRE ATT&CK takes cyber defense planning and preparation to the edge of what is possible today.

The reason for this growth in adoption is simple: the use of cybersecurity and information technology frameworks is compelling. Frameworks give you a top level plan to organize governance, build out a highly functional organization, address threats and challenges, and more. Many organizations have difficulty with using these frameworks in practice. How do you operationalize frameworks in a way that can provide rapid tangible benefits?

To illustrate how quickly you can get a framework into operation, this report will share a best practice example of how to rapidly and effectively operationalize MITRE ATT&CK. MITRE ATT&CK is a specialized framework that helps organizations directly address and defeat the tactics, techniques, and procedures (TTPs) of the most sophisticated cyber attackers. MITRE ATT&CK is complementary to these other major frameworks and works well with automated approaches.

Once you have operationalized MITRE ATT&CK, you will be able to answer difficult questions about the performance of your security controls as configured and your ability to mitigate new and emerging threats.

All of these frameworks provide a set of guidelines, standards, and best practices to reduce enterprise risk. Frameworks give managers a reliable and battle-tested way to use best practices that help align information technology and cybersecurity management and governance to the enterprise goals.

In some cases cybersecurity frameworks are mandatory, based upon compliance and regulatory requirements. Some may be mandated by the government, others, by private industry consortiums. For example, if you want to use credit cards in the United States to handle financial transactions in your business, you will need to be in alignment with the PCI-DSS standard. Other major compliance regulations, such as HIPAA, GDPR, and NERC CIP, bring their own well-defined cybersecurity frameworks requirements.

[1] https://static.tenable.com/marketing/tenable-csf-report.pdf

Frameworks - The Big Picture

There are many different types of frameworks in use worldwide. Frameworks often serve different purposes, and one organization will typically adopt and utilize more than one. Critical in this cyberthreat-rich environment are those frameworks that focus on attacker tactics, techniques, and procedures (TTPs). Understanding the mind of the attacker is important to building and validating the best cyber defense.

Cybersecurity is a major driver for framework adoption. Compliance regulations also bring mandatory cybersecurity frameworks which are also key drivers. Some of the frameworks are designed to help you design, organize, deploy, and manage a complete information technology and cybersecurity architecture. Others focus on one area or industry, such as banking and finance for PCI-DSS or healthcare for HIPAA.

You will note that we classify compliance regulations such as GDPR and HIPAA as frameworks because they specify detailed approaches to the protection of data and the corresponding IT infrastructure and security controls. Others focus on top level strategy, such as Zero Trust. Zero Trust is an important cyber defense strategy that supplements and evolves past the basics of defense in depth.

Please reference Appendix A to see the additional list of frameworks we reviewed.

Table - The Top Six Leading Cybersecurity Frameworks

Framework	Description	Direct Link
ISO 27001/27002	ISO/IEC 27001/27002 is a widely deployed framework and standard providing requirements for an information security management system (ISMS), though there are many more standards in the ISO/IEC 27000 family.	https://www.iso.org/isoiec-27001-information-security.html
CIS-CSC	IT security leaders use CIS Controls® to quickly establish cyber defenses for their organizations. CIS Controls brings a series of 20 foundational and advanced cybersecurity actions that enable you to defeat the most common attacks.	https://www.cisecurity.org/controls/cis-controls-list/
NIST CSF	The NIST (National Institute of Standards Technology) Cybersecurity Framework is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices. In 2013, the president issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which resulted in the creation of CSF.	https://www.nist.gov/cyberframework/new-framework
ISACA COBIT 2019 (prior version COBIT 5)	COBIT® (Control Objectives for Information and Related Technology) is ISACA®'s IT management framework to help companies develop, organize, and implement strategies around information and governance.	https://www.isaca.org/resources/cobit
Lockheed Martin Cyber Kill Chain	The Lockheed Martin Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions. The model identifies what the adversaries must complete in order to achieve their objective — it is a view into the activities of the attacker.	https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
MITRE ATT&CK	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.	https://attack.mitre.org/

The ISO 27001 Standard Framework for ISMS Deployment

ISO 27001 is part of a series of standards that enables organizations to better manage and protect their sensitive data and reduce risk. At the 1,000-foot view, ISO 27001 helps you organize and deploy a comprehensive information security management infrastructure. Critical components include the mechanisms and best practices you use to secure your networks, IT assets, and sensitive information to lower overall vulnerability. ISO 27001 shares everything you need to know to build out your security controls, personnel, and processes to organize your security from top to bottom.

The ISO 27001 standard is a compendium of best practices to support the design, deployment, and management of an Information Systems Management System (ISMS). An ISMS puts into production the cybersecurity framework which will address the mitigation and reduction of cybersecurity risks.

ISO 27001 is highly scalable and can work with any type of organization, including government as well as commercial enterprise. At a conceptual level, ISO 27001 does not spell out specific security controls but instead links to the important companion standard, ISO 27002, which includes more detailed guidance on the best practices to build out a complete ISMS and provides more data on specific security controls.

The ISO® organization (International Organization for Standardization) includes representatives from over 150 national standards organizations. These representatives come together to build consensus and deliver international standards to help support product safety and development.

As we drill in, we will see that ISO 27001 consists of 14 security control clauses. These security control clauses in turn contain 35 main security categories and 114 controls (as of ISO/IEC 17001:2013). In terms of the structure, security control categories spell out the objectives and the corresponding security controls that can support reaching these objectives. Annex A of the ISO 27001 standard provides a view of the security controls organized by clause, category, and the security controls in a category.

Table - ISO 27001 Organization

Section 1, 2, and 3	Introduction regarding terminology and references
Section 4	Define scope of an ISMS and provide for continuous process improvement
Section 5	Defines leadership, policies, and organizational relationships
Section 6	Defines plans for risk management, planning milestones, and related processes
Section 7	Defines the important team personnel resources that are required for an ISMS
Section 8	Defines operational issues and planning to address risk objectives, defined earlier in section 6
Section 9	Defines the requirements for management audit and review, and setting metrics for performance of the ISMS
Section 10	Defines continuous process improvement as an iterative cycle
Annex A	Details on security controls: 14 clauses, 35 categories, 114 controls

Table 2 - ISO 27001 Annex A Organization

Annex A	Clauses - 14	Category - 35 Total	Controls - 114 Total
A.5	Information Security Policy	1	2
A.6	Information Security Organization	2	7
A.7	Human Resources	3	6
A.8	Asset Management	3	10
A.9	Access control	4	14
A.10	Cryptography	1	2
A.11	Physical and Environmental Security	2	15
A.12	Operational Security	7	14
A.13	Communications Security	2	7
A.14	System Acquisition, Maintenance, and Development	3	13
A.15	Supplier Relations	2	5
A.16	Incident Management	1	7
A.17	Business Continuity Management	2	4
A.18	Compliance	2	8

ISO 27001 (and the related ISO 27002) enables CISOs to build out a highly competent cybersecurity framework that can substantially improve cyber defense and reduce overall business risk. Implementing an information security management system by following the ISO 27001 model will provide your enterprise with a system that will help to minimize the risk of security breach.

An effective ISO 27001 information security management system provides a management framework of policies and procedures that will help your organization keep your networks and data secure. By developing and maintaining a well structured and documented system of controls and management, risks can be identified and reduced.

The CIS-CSC Cybersecurity Framework

The Center for Internet Security®'s Critical Security Controls Framework was released by the SANS Institute over 10 years ago. Initially, this was called the Consensus Audit Guidelines and has since been referred to as the CIS-CSC, CIS Controls®, and the SANS Top 20. The framework was ultimately adopted by the Center for Internet Security in 2015.

The CIS CSC framework is popular and has been adopted by over 30 percent of major organizations worldwide. The CIS Controls framework supports and builds upon the idea that "offense informs defense." Data from actual attacks is used to assemble the CIS controls database to improve cybersecurity resiliency and effectiveness.

Table - Five Key CIS Controls Factors

Facor 1	Offense informs defense
Facor 2	Prioritization of the security controls that provide the best risk reduction and protect against your expected threats
Facor 2	Common and shared metrics so that all the effectiveness of security controls can be measured and understood
Facor 2	Measurement and mitigation — are the current security controls performing as you expect?
Facor 2	Automation is required to achieve scale and reliable measurements to validate security controls performance under CIS

The CIS Controls framework is organized around 20 security controls. This also includes sub-controls as required. All of this is focused on positioning known best practices against the threats which your enterprise is expected to face.

Prior to implementing CIS Controls, you must review the characteristics of your organization against the profile assigned to each of three implementation groups. You must also perform a risk assessment using the CIS risk assessment model.

Table - CIS Implementation Groups

IG1 Implementation Group	Less than perhaps 10 employees
IG2 Implementation Group	Larger organization more geographically distributed
IG3 Implementation Group	Enterprise or government with 1000s of employees might self classify as an IG3

This, in turn provides, guidance as to which CIS Controls should be used by your organization. CIS Controls are defined by category:

- Basic controls are essential for any organization
- Foundation controls provide security best practices
- Organizational controls add more structure to people and related process execution

Table - CIS Security Controls for Basic, Foundational, and Organizational

Basic Controls	Foundational Controls	Organizational Controls
1 - Inventory and control of hw assets	7 - Web browser and email	17 - Security training
2 - Inventory of sw assets	8 - Malware cyberdefense	18 - Application sw security
3 - Vulnerability management	9 - Control of network ports, services, and protocols	19 - Incident response
4 - Control of admin privileges	10 - Data recovery capabilities	20 - Penetration tests and red team exercises
5 - Secure configurations for hardware platforms	11- Secure configurations for network devices, firewalls, and routers	
	12 - Boundary cyberdefense	
	13 - Data protection	
	14- Controlled access - need to know	
	15 - Wireless access controls	
	26 - Account monitoring and control	

The CIS Controls framework is a useful guide for CISOs to improve cyber defenses and reduce overall cyber risk. CIS Controls is focused on stopping the most likely attacks. It helps you prioritize controls to help minimize risk for the resource mix you have. The critical security controls are generally based on the most likely attacks as derived from the most current threat intelligence reporting. These are validated by government and industry experts, and the critical security controls are updated as soon as security researchers analyze the data and provide new recommendations.

The NIST Cybersecurity Framework

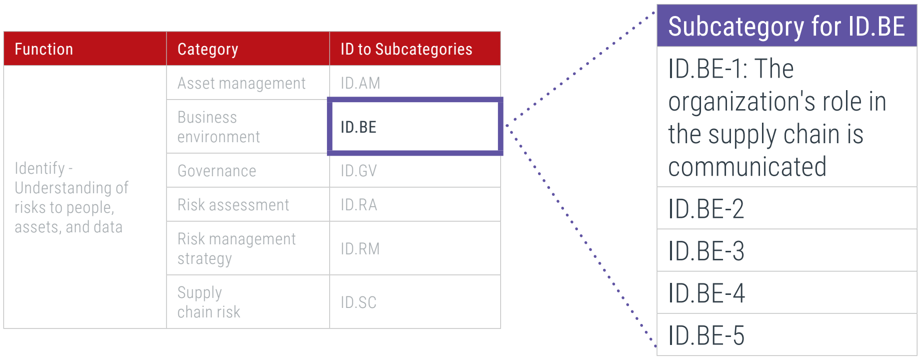
The National Institute of Standards and Technologies (NIST) Cyber Security Framework (CSF) is a definitive set of best practices and well defined standards that CISOs can adopt to improve their overall cyber defenses and reduce their risk. The NIST CSF allows government and commercial enterprises to more capably manage cybersecurity risks. The adoption of this framework is voluntary. It can also coexist with other frameworks such as ISO 27001, ISACA COBIT, and others.

The NIST CSF consists of five high-level core components that, in turn, consist of 23 categories and 108 subcategories. The Core is a set of desired cybersecurity activities and outcomes organized into Categories and aligned to Informative References. The Framework Core is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language. The Core consists of three parts: Functions, Categories, and Subcategories. The Core includes five high-level functions: Identify, Protect, Detect, Respond, and Recover. These five functions are not only applicable to cybersecurity risk management, but also to risk management at large. The next level down is the 23 Categories that are split across the five Functions. The image below depicts the Framework Core's Functions and Categories.

Table - NIST Core Functionality

Function	Category	ID to Subcategories
Identify - Understanding of risks to people, assets, and data	Asset management	ID.AM
	Business environment	ID.BE
	Governance	ID.GV
	Risk assessment	ID.RA
	Risk management strategy	ID.RM
	Supply chain risk	ID.SC
Protect - Implement the best security controls for data security, access control, and identity management	Identity management & access control	PR.AC
	Training	PR.AT
	Data protection	PR.DS
	Information protection	PR.IP
	Maintenance	PR.MA
	Protective technology	PR.PT
Detect - Implement anomaly detection, threat intelligence, and extensive monitoring and logging	Anomalies and events	DE.AE
	Security continuous monitoring	DE.CM
	Detection processes	DE.DP
Respond - Respond to and mitigate security events with orchestration and playbooks	Response planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	14- Controlled access - need to know
Recover - Plans for recovery after a disabling or impairing cyber attack	Recovery planning	14- Controlled access - need to know
	Improvements	14- Controlled access - need to know
	Communications	14- Controlled access - need to know

Table - NIST Category Expansion Example by ID to Subcategory



Function	Category	ID to Subcategories
Identify - Understanding of risks to people, assets, and data	Asset management	ID.AM
	Business environment	ID.BE
	Governance	ID.GV
	Risk assessment	ID.RA
	Risk management strategy	ID.RM
	Supply chain risk	ID.SC

Subcategory for ID.BE
ID.BE-1: The organization's role in the supply chain is communicated
ID.BE-2
ID.BE-3
ID.BE-4
ID.BE-5

The five subcategories pictured from the Business Environment Category (ID.BE) in the chart above provide an example of outcome-directed goals. There is another column not shown in the above chart that would be to the right. This column, Informative References, provides references to other standards such as ISO27001, COBIT 5, NIST SP 800-53, and others.

NIST implementation tiers helps organizations categorize their operating processes into four tiers: 1 - Partial, 2 - Risk Informed, 3 - Repeatable, and 4 - Adaptive. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor, how well integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity information from external parties.

If a risk assessment determines that not all potential endpoint devices are in the database, this would be classified as 1 - Partial, identifying it for improvement.

Profiles represent the organization's assessment of its organizational requirements and objectives, trade-offs against risk, and resources available against the targeted outcomes in the NIST Framework Core. Profiles can compare a "Current" Profile with a "Target" Profile to maintain focus on improvement. Profiles help an organization optimize its cybersecurity framework to best protect the organization.

The creation and gap analysis of these profiles helps an enterprise prioritize their implementation planning and execution. The priority, work required, and estimated cost of remediation and improvement help the enterprise plan and budget necessary cybersecurity activity.

The NIST CSF Framework provides a standard language that all stakeholders can understand and a highly systematic methodology. NIST CSF includes suggested activities that can be incorporated in a cybersecurity program which can meet any commercial or government enterprise needs. NIST CSF is designed to complement existing enterprise cybersecurity programs and risk management processes.

The ISACA®'s COBIT® Cybersecurity Framework

The Control Objectives for Information and Related Technologies (COBIT) is the IT and cybersecurity management framework first released nearly 25 years ago by the Information Systems Audit and Control Association (ISACA). The first release was in 1996 as an early audit support tool. After several releases, this has resulted in COBIT 2019. Today, COBIT 2019 provides a robust and well-tested framework for governance and the management of enterprise information technology across the largest enterprises in the world. The goal of COBIT is to help align enterprise business objectives with information technology and cybersecurity goals by defining processes that can close the gaps between all of these organizations.

COBIT 2019 substantially upgrades the framework for both enterprise and government by directly addressing current technologies and, most importantly, current cybersecurity trends. COBIT 2019 has a heavy emphasis on security and risk management as well as associated information governance. The biggest differences between COBIT 2019 and the previous version, COBIT 5, include the expansion from five to six governance principles, 37 to 40 processes, and the addition of governance framework principles.

COBIT 2019 Publications include:

- COBIT 2019 Framework - Introduction and Methodology. The COBIT 2019 framework overviews the governance principles and key concepts. This guide presents the structure of the overall framework and the COBIT Core Model.
- COBIT 2019 Framework - Governance and Management Objectives. This publication provides a description of the COBIT Core Model and all of the 40 governance and management objectives which it contains. Objectives map to the related process, goals, and governance, and management practices.
- COBIT 2019 Design Guide. The new COBIT 2019 design guide provides direction on how to put COBIT into use and how to build out a governance system to any enterprise's needs, defining and explaining various design factors.
- COBIT 2019 Implementation Guide. The COBIT 2019 Implementation Guide provides a path for continuous improvement on governance needs.

COBIT 2019 has six basic governance system principles, expanding and redefining the five governance principles in COBIT 5. These include:

- Provide stakeholder value;
- Holistic approach;
- Dynamic governance system;
- Governance distinct from management;
- Tailored to the enterprise needs; and,
- End-to-end governance system.

Governance framework principles have also been added to COBIT 2019. This includes:

- A conceptual model — this is to identify key components and relationships among the components to maximize consistency and enable automation.
- Open and flexible — this calls out the addition of new content and the ability to address new issues in a flexible way.
- Aligned to major standards — this third principle notes that the model should be in alignment with major frameworks, standards, and regulations.

The use of COBIT 2019 is considered compelling by many of their users. The expanded focus of COBIT 2019 brings many important new features and addresses current governance topics such as small and medium businesses, digital transformation and the risks it brings, cloud computing, data privacy, cybersecurity, and securing the devops cycle.

COBIT 2019 delivers considerable capability and advantage to any enterprise. It is simple, easy to use, flexible, and it supports many different types of enterprise and threat environments. It provides one of the best common platforms for enterprise leadership to use for communications about information technology related goals and results. COBIT 2019 also provides a best practices path to optimize cyber defense environments, so as to mitigate the ongoing cyber threats faced today.

The Lockheed Martin Cyber Kill Chain®

The Lockheed Martin Cyber Kill Chain is an adaption of the military kill chain concept to cybersecurity. The Kill Chain is an excellent way to model intrusions on a computer network when it was first announced in 2011. The seven steps in the Kill Chain help defenders better model and understand the potential threat activity. It then helps them improve defenses to meet and mitigate these evolving threats. The Kill Chain also provided clarity to the taxonomy of attacker activity at a time when advanced attacker TTP-based frameworks, such as MITRE ATT&CK (which was officially released in 2015) were not available.

Table - The Seven Steps in Lockheed Martin Cyber Kill Chain

Kill Chain Step	Description
Reconnaissance	Reconnaissance often includes preparing and gathering data for social engineering, the acquisition of email addresses, knowledge of frequented websites, and more. This first step includes target selection. Attackers seek to blueprint the targeted IT systems and see vulnerabilities that can be used to support this exploit and breach. The longer the attacker is hidden within the network, the more likely they are to succeed.
Weaponization	Now that the attackers have finalized their plan, they will couple the exploit with a backdoor into a deliverable payload targeted for that use. Often this involves the modification of existing malware to support the attack. The malware and techniques of sophisticated attackers may take advantage of zero-day exploits (not previously known), or some mix of vulnerabilities to get around enterprise defenses.
Delivery	Email remains the attack vector of choice for weaponized payload delivery. This is followed by malware-laced websites or maladvertisements that they might display, as well as malware-laced removable media such as USB memory.
Exploitation	The vulnerability is now exploited to execute code within the target enterprise.
Installation	Malware is installed. Now a specialized software which provides a "backdoor" allows the attacker to maintain persistence in the target environment.
Command & Control	Command and control channels are set up and are now used to provide the attacker with relatively unfettered remote access to their objectives within the network.
Actions on Objectives	Attackers use their access to accomplish their original goals, which may include data theft, exfiltration of funds, destruction of enterprise assets, and more.

Today, the Kill Chain is part of Lockheed Martin's bigger vision for Intelligence Driven Defense®. Intelligence Driven Defense is strategy which focuses resources on stopping the offensive activity of a cyber attack while maintaining a strong defensive posture. Attackers are constantly evolving their tactics, techniques, and procedures — the defenders need to do so at a faster pace. Lockheed Martin's five components of Intelligence Driven Defense speak to:

- Centralized operations to focus the organization;
- Monitoring of threats to provide continual situational awareness;
- Management of actionable intelligence;
- Proactive defense to mitigate offensive activity; and,
- Measurement of success for accountability, assessment, and lessons learned.

In mapping out the attacker's activity in a cyber attack using the Cyber Kill Chain, security operations analysts can more rapidly identify the steps where this Kill Chain can be broken as the attack unfolds. This is all about anticipating the next moves of the attacker and shutting the attack down. For this reason, the use of the LockHeed Martin Cyber Kill Chain framework has been compelling and remains a basic tool for most SOC analysts worldwide.

The MITRE ATT&CK® Cybersecurity Framework

MITRE ATT&CK is, in both depth and breadth, the largest attack knowledge base providing suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the Kill Chain to include the widest variety of tactics; these tactics are then supported by detailed techniques. This organized approach enables you to methodically select and analyze attacks and to compare them to the capabilities of your security controls in order to understand the gaps. Once understood, you can then rationally expand your security controls and adjust your budgets.

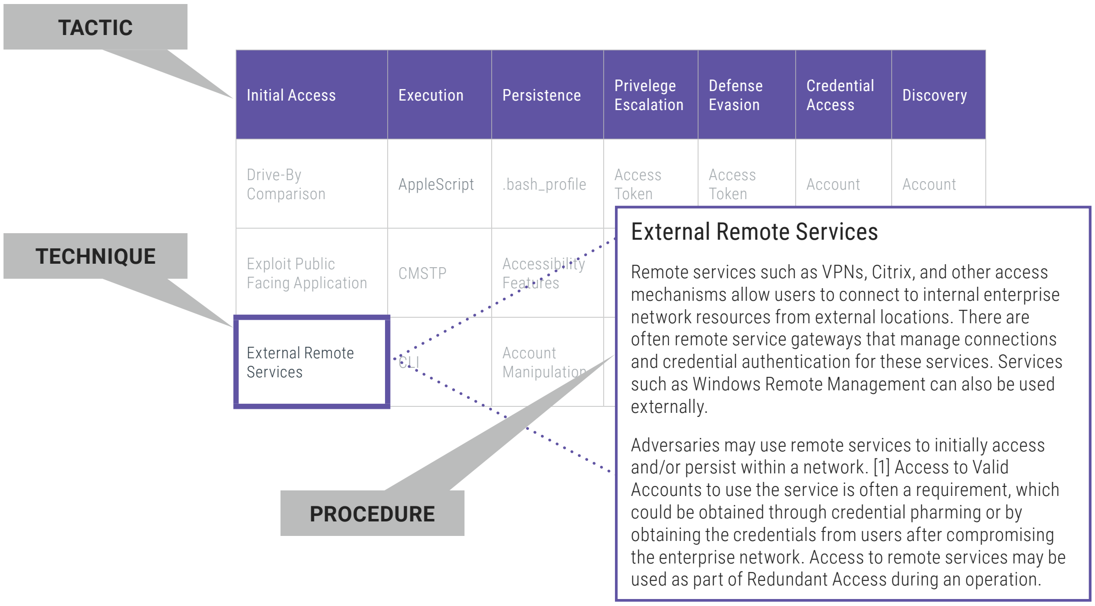
With MITRE ATT&CK, you can review your security controls and gain visibility into gaps in your defenses. Security management can rapidly and easily identify critical problems for remediation. This objective assessment provides a data-driven approach to prioritizing and scaling your cybersecurity program and budget.

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. This provides, for the first time, a common lexicon that enables stakeholders, cyber defenders, and vendors to clearly communicate on the exact nature of a threat and the objective assessment of the cyber defense plan that can defeat it. This common lexicon brings a universal language that can be used to describe the procedures of an attacker or attack tools and exactly the techniques which they deploy. The precise lexicon of MITRE ATT&CK enables more precise assessment of threats and a faster, better-targeted response.

The MITRE ATT&CK Matrix for Enterprise provides a complete view to all of the attacker techniques for Windows, Linus, and MAC. Each of the 12 tactics (columns) include from between nine to 67 techniques. Note that many techniques are used by multiple tactics. You can get a sense of this organization based upon the Table below.

Tactics define the specific goals of the attacker. For example, one primary tactic is Privilege Execution. The Privilege Execution Tactic column includes all of the techniques that an attacker might use to try and gain higher-level permissions that would then be used, in turn, to compromise your defenses.

Table - The MITRE ATT&CK Matrix



Initial Access	Execution	Persistence	Privelege Escalation	Defense Evasion	Credential Access	Discovery
Drive-By Comparison	AppleScript	.bash_profile	Access Token	Access Token	Account	Account
Exploit Public Facing Application	CMSTP	Accessibility Features				
External Remote Services	CLI	Account Manipulation				

External Remote Services

Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.

Adversaries may use remote services to initially access and/or persist within a network. [1] Access to Valid Accounts to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network. Access to remote services may be used as part of Redundant Access during an operation.

MITRE ATT&CK Groups help you identify attackers more precisely. This database shows you all of the known names and suspected identifies of attackers. Importantly, it also shows you which techniques and software tools are attributed to the different attacker groups. This section has 90-plus groups defined and continues to grow as more threats are identified. Note that this data is not necessarily complete — it is as available based upon the sources that MITRE monitors on an ongoing basis.

Operationalize Your Cybersecurity Framework - Start With MITRE ATT&CK

Why MITRE ATT&CK?

MITRE ATT&CK complements just about every information technology and cybersecurity framework in use today. MITRE ATT&CK adds significant value as it focuses on the tactics, techniques, and procedures of the attackers. It enables your team to better understand the mind of an attacker to better defend your enterprise. By operationalizing MITRE ATT&CK, you can know the answer to the toughest questions and more:

- Are my security controls working as we expect?
- How can I assess and reduce risk?
- Am I optimizing the value from my security controls expenditures?
- Are we protected against a likely threat to my enterprise and industry such as APT29? Can I model this exactly?

MITRE ATT&CK is an excellent place to start to bolster your cyber defenses, reduce risk, and objectively assess the performance of your security controls. Once again, it is highly complementary to every other framework, especially widely used frameworks such as ISO 27001, NIST CSF, CIS-CSC, ISACA's COBIT 5, and ISACA COBIT 2019. You can start with one or more of these in place, or you can add these later. MITRE ATT&CK is a great place to start and can help you begin reducing risk immediately.

Operationalize MITRE ATT&CK with a Breach and Attack Simulation Platform

The fastest and simplest path to operationalizing MITRE ATT&CK is to deploy a breach and attack simulation (BAS) platform. BAS technology allows enterprises to rapidly and automatically implement the MITRE ATT&CK framework. You will quickly be able to simulate the full attack and expanded kill chain used by cyber attackers against enterprise infrastructure by using software agents, virtual machines, and other means. BAS also allows you to understand the detailed status and performance of your security controls and processes, along with the personnel that support them. You will be able to find the performance gaps, strengthen your security posture, and improve your incident response capabilities. BAS automation of the MITRE ATT&CK framework confirms readiness and validates that your enterprise security systems are performing as originally intended.

BAS platforms provide automation that enables the platforms to work autonomously and to scale to support the largest global enterprise. Support for live production environments enables you to see in real time how changes to configurations or administration can open new vulnerabilities in your cyber defense. This is vital, as these are frequent sources of vulnerabilities discoverable by cyber attackers.

How Do You Get Started With a BAS Platform?

There are many ways to rapidly reduce risk and derive return on investment from your MITRE ATT&CK investment. These include validating basic security control performance, leveraging threat intelligence to better assess your exposure, and determining how your cybersecurity defense stack will perform against different attacker behaviors. Let's take a closer look at this quick start guide to operationalizing MITRE ATT&CK.

Validating Security Control Performance

You can use the MITRE ATT&CK tactics and techniques to help you both measure the efficacy and configurations of your security controls and validate their performance against your assumptions. Security control categories might include data loss prevention (DLP), endpoint detection and response (EDR), web filtering, firewalls, and more.

This valuable capability allows you to immediately validate that your security controls are configured correctly, performing as expected, and delivering the return on investment that you expect. The goal is to keep it simple. The average enterprise may have as many as 75 security products, so it helps to start by prioritizing this list and selecting the first five that are highly critical to your business operations.

For example, firewalls are fundamental to your security stack. BAS will enable you to test this important control, including network segmentation, application control policy enforcement, and malware protection. Another important category you might select is EDR, where you similarly could test suspicious and/or anomalous endpoint activities.

By using BAS to complete end-to-end testing of critical areas for which you assume you have defensive coverage, you will be equipped with objective data in the form of a report to present to your team to prioritize remediation of gaps. This report can also be shared with management and other business units within your organization to communicate the state of your security posture.

Better Leveraging Threat Intelligence

Threat intelligence programs develop from the experience your organization has gained from internal events as well as the data you may acquire externally. Threat intelligence data is dynamic — it is constantly changing based upon your experience. The MITRE ATT&CK knowledge base enables you to turn your tactical experience into a strategic threat intelligence capability.

If your security program is mature and you have implemented a threat intelligence program with a dedicated team within your organization, you can leverage that intelligence within the BAS platform. This can include knowledge of past breaches that your organization has withstood and likely attacks that you expect might occur given external intelligence information.

Model the Most Recent and Sophisticated Attacks

By operationalizing MITRE ATT&CK, you can determine if your cyber defenses can stand up to the most recent and sophisticated attacks. You will know if your existing cybersecurity stack will detect and prevent it and if your security operations team will be able to respond to such a combination of attack techniques effectively. You will be enabled to objectively test your cyber defense strategy, security controls, and supporting procedures and personnel.

Recommendations and Conclusions

It is now industry best practice to implement and deploy one or more information technology and cybersecurity frameworks. Frameworks provide substantial value in support of your efforts to better utilize resources, successfully meet the current wave of cyber threats, and reduce risk.

As you implement your chosen frameworks, consider the operationalization of MITRE ATT&CK supported by the automation of a breach and attack simulation platform. A BAS platform will validate the real-time production performance of your security controls, better integrate threat intelligence, and help you understand the ability of your defenses to meet (and defeat) new and emerging threats.

About AttackIQ and Informed Defense

AttackIQ®, a leader in the breach and attack simulation market, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ provides comprehensive support for the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected.

The AttackIQ Informed Defense Architecture (AIDA) enables a transparent and completely manageable attacker kill chain testing methodology. By combining the ability to emulate attacker behavior in the early stages of attack, lateral movement behaviors through communication between test points, and using current and highly integrated network threat packet captures; AIDA affords the most comprehensive automated security testing platform available.

The AttackIQ Informed Defense solution is built on an industry-first unified architecture that:

- Allows security teams to take advantage of the most comprehensively MITRE ATT&CK-aligned library of known attacker tactics, techniques, and procedures (TTPs) and includes an open platform that enables these TTPs to be tailored or tester defined.
- Provides an integrated testing architecture that allows customers to closely emulate threat actor behaviors across the entire adversary kill chain. From execution to defense evasion, from credential access to lateral movement, even including attackers living off the land.
- Invokes the integration of commercially-available network packet capture of threat behaviors that can be passed between these test points which best exercises internal segmentation strategies.
- Includes external orchestration infrastructure that integrates the ability to test organizational boundary security controls.

Combined with the company's open system testing approach and validation tests for enterprise and cloud, the AttackIQ Informed Defense solution ensures that customers and partners have the right content and testing methodology at their fingertips. AttackIQ's mission is to help organizations continuously optimize their security programs' effectiveness. The best way to do this is with a unified architecture that can test from a point of breach and test in-line security controls in production, at scale, safely. These are two different requirements. Security teams need to be able to do both.

AttackIQ Informed Defense's new solution features include:

- The ability to promote existing AttackIQ test points staged throughout the production environment to become traffic-replay capable.
- Intelligent PCAP session replay across inline network devices.
- Modular infrastructure in service provider cloud IaaS networks that can play the role of an internet-based entity or target for PCAP replay.
- Options to add internet-based roles for geo-testing.
- Validation of internal security boundaries by using existing systems without having to deploy virtual machines.
- PCAP library updates with examples of latest malware infections, command and control communications, and other test-ready samples.

AttackIQ Academy

Customers and partners are welcome to learn how to operationalize MITRE ATT&CK, unlock purple-teaming, and evolve their security programs into Threat Informed Defense practices by joining the AttackIQ Academy.

Courses are free to attend. To register, visit: https://attackiq.com/academy/.

Appendix A

Table - Additional Cybersecurity Frameworks

Framework	Description	Direct Link
NIST 800-53	NIST SP 800-53 database represents the security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations.	https://nvd.nist.gov/800-53
NIST SP 800-12	This publication introduces the information security principles that organizations may leverage to understand the information security needs of their respective systems.	https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
FEDRAMP	The Federal Risk and Authorization management Program (FedRAMP) is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services.	https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf
IASME Governance	A governance security standard developed by the UK government.	https://iasme.co.uk/
SOC 2®	The American Institute of Certified Public Accountants (AICPA®) developed the SOC 2 framework. SOC 2 overviews an auditing process that ensures your service providers securely manage your data. This is both to protect your enterprise and the privacy of your clients.	https://www.aicpastore.com/AuditAttest/IndustryspecificGuidance/soc-2-sup--reg---sup--reporting-on-an-examination-/PRDOVR~PC-0128210/PC-0128210.jsp?icid=hp-publications:recs:clicked:SOC+2%C2%AE+Reporting+on+an+Examination+of+Controls+at+a+Service+...:PC-0128210
ETSI TC Cyber	ETSI TR 203-305-x series of reports define a framework which overviews a defense-in-depth set of best practices that mitigate the most common cyber attacks against enterprise infrastructure.	https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf
GDPR	The General Data Protection Regulation (GDPR) is the toughest privacy and cybersecurity law in the world. Though it was drafted and passed by the European Union, it imposes obligations onto organizations everywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.	https://gdpr.eu/
HIPAA	The Health Insurance Portability and Accountability Act of 1995 (HIPAA) regulatory framework describes the protections required for sensitive healthcare information and provides corresponding direction with respect to cybersecurity controls and procedures.	https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
HITRUST CSF®	The Health Information Trust Alliance developed the Common Security Framework for healthcare organizations. These guidelines cover any information systems that work with protected health information to minimize risk and to improve overall cyber defense.	https://hitrustalliance.net/hitrust-csf/
PCI-DSS	The PCI-DSS security framework defines payment security is required for all entities that store, process or transmit cardholder data. These set the requirements for organizations accepting or processing payment transactions and for software developers and manufacturers of applications and devices used in those transactions.	https://www.pcisecuritystandards.org/
COSO.org	The Enterprise Risk Management Integrated Framework highlights the importance of considering risk in both the strategy-setting process and in driving performance. The first part shares best practices on current and evolving concepts and applications of enterprise risk management. The second part, the framework, is organized into five components that can fit many types of operating structures, and enhance strategies and decision-making to reduce risk.	https://www.coso.org/Pages/default.aspx

Framework	Description	Direct Link
ITIL®	ITIL is a framework for IT Service Management practices. The British standard 15000 and the subsequent ISO/IEC 20000 Service Management standard are based on the ITIL framework. ITIL was developed by the British government's Central Computer and Telecommunications Agency (CCTA) in the 1980s and has evolved quite a bit. It is now licensed by Axelos.	https://www.axelos.com/best-practice-solutions/itil
FISMA	The Federal Information Security Modernization Act of 2014 (FISMA 2014) updates the Federal Government's cybersecurity practices by codifying the Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems.	https://www.cisa.gov/federal-information-security-modernization-act
NERC CIP	The NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) plan is a framework that is designed to secure the critical assets essential for operating North America's power system	https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
NYDFS Cybersecurity Regulation	The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a set of regulations from the NY Department of Financial Services (NYDFS) that places cybersecurity requirements on applicable financial institutions.	https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
SCAP	The Security Content Automation Protocol (SCAP) defines standards to enable vulnerability management, measurement, and policy compliance evaluation of systems. NIST publishes The Technical Specification for the Security Content Automation Protocol (SCAP) (NIST SP 800-126 Rev. 3) and an annex to this publication, SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3.	https://csrc.nist.gov/projects/security-content-automation-protocol/
NCSC 10 Steps	The 10 Steps to Cyber Security was originally published in 2012 and is now used by a majority of the FTSE 350. The 10 steps guidance is complemented by the paper Common Cyber Attacks: Reducing The Impact.	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
Zero Trust	Originally proposed by Forrester in 2009, this has evolved considerably with cross-vendor industry support into a comprehensive strategy for improving cyber defense and reducing risk.	https://go.forrester.com/government-solutions/zero-trust/

ATTACKIQ
U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. With an open platform, AttackIQ supports the MITRE ATT&CK framework, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying defenses work as expected. AttackIQ's platform is trusted by leading companies around the world.
For more information visit: www.attackiq.com. Or follow AttackIQ on Twitter, Facebook, LinkedIn, Vimeo, and YouTube.