Security vs Compliance

Striking the Right Balance

Dave Hatter, CISSP, CISA, CISM,CCSP, CSSLP, Security +, Network+, PMP, ITIL

Director of Business Growth

Intrust IT

IT NATION™ SECURE

Agenda

Define security and compliance

Understand security

Understand compliance

Compliance standards

Strategy

Q&A

THE WHITE HOUSE

MENU

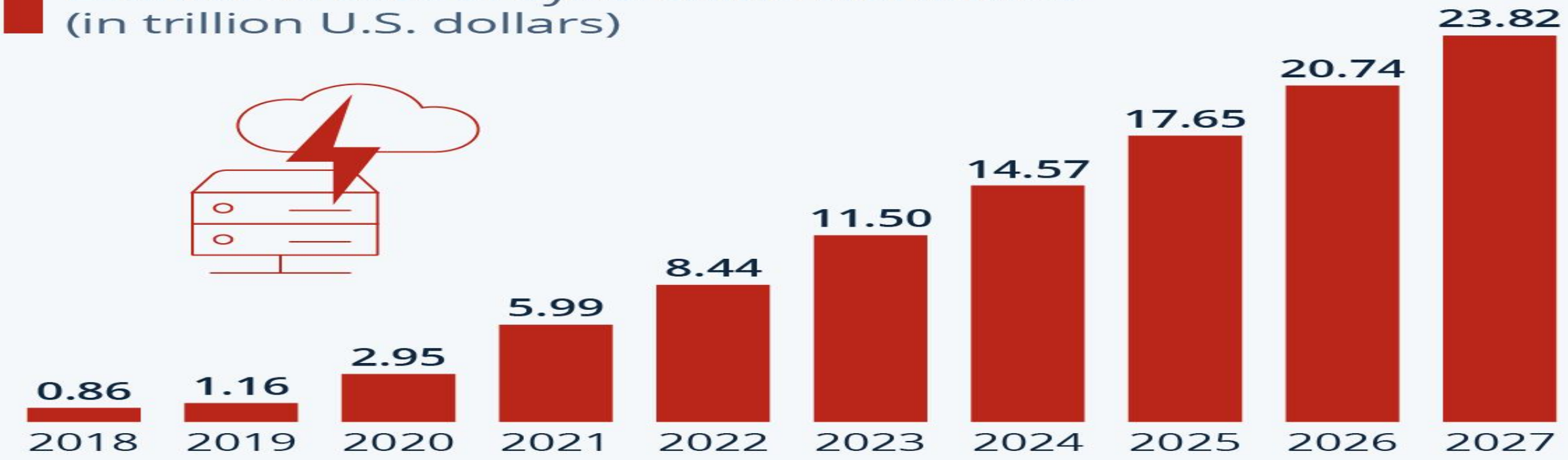
BRIEFING ROOM

FACT SHEET: Act Now to Protect Against Potential Cyberattacks

MARCH 21, 2022 • STATEMENTS AND RELEASES

Cybercrime Expected To Skyrocket in the Coming Years

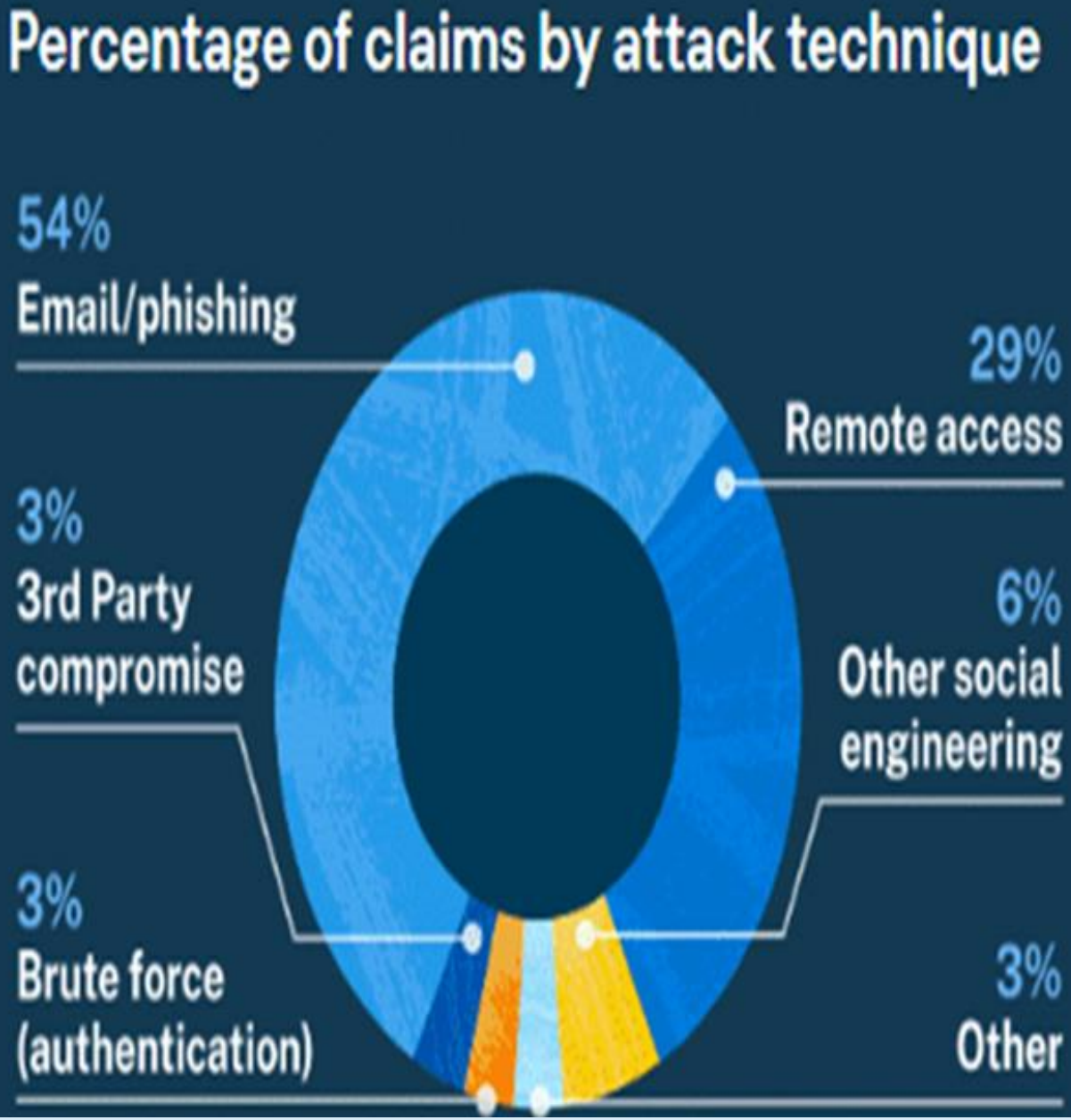
Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

statista


Most common cyber incidents (% of reported claims)
Ransomware
41%
Funds transfer fraud
27%
Email compromise
19%
Other
13%
0%
10%
20%
30%
40%
50%


Percentage of claims by attack technique
54%
Email/phishing
29%
Remote access
3%
3rd Party compromise
6%
Other social engineering
3%
Brute force (authentication)
3%
Other

Industries Affected

23% Healthcare (including Biotech & Pharma)

17% Business & Professional Services (including Engineering & Transportation)

15% Finance & Insurance

12% Education

10% Manufacturing

9% Retail, Restaurant & Hospitality

6% Government

4% Nonprofit

2% Technology

2% Energy

Futurism

INTENT TO KILL | 4:50 PM *by* VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."


WE ARE NO LONGER
SECURING COMPUTERS
WE ARE SECURING SOCIETY.

Security vs Compliance

- Often intertwined and closely related, **but not the same thing**
- Compliance measures may help ensure an organization meets certain security requirements **but does not guarantee an organization is fully protected from all potential threats**
- Security measures without considering compliance requirements can leave an organization vulnerable to legal and regulatory penalties
- Just checking the “compliance box” is often not enough to defend organizations from rapidly changing threats

Security

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing a range of technical, administrative, and physical **controls** to safeguard against potential threats and vulnerabilities.

Security

- Proactive ongoing process
- Emphasizes the protection of information assets from internal and external threats
- Objective is to:
  - Prevent, detect, and respond to security incidents
  - Minimize the impact of potential breaches or attacks
- Involves implementing various technical controls
- Often done in a piecemeal fashion
- Often focused on tools and “solutioning”

Security Control

A measure or mechanism put in place to reduce the risk of a security threat, vulnerability, or attack. They protect the confidentiality, integrity, and availability (CIA) of information and systems and reduce or eliminate threats and vulnerabilities that could lead to unauthorized access, use, disclosure, disruption, modification, or destruction of data or systems.

CIA Triad

Security Controls

Physical

- Locks
- Fences
- Cameras
- Biometrics
- Guards
- Background Checks

Technical

- IAM
- Authentication
- EDR/MDR/XDR
- Firewalls
- IDS/IPS
- SIEM
- MFA
- Patching
- Segmentation
- Encryption

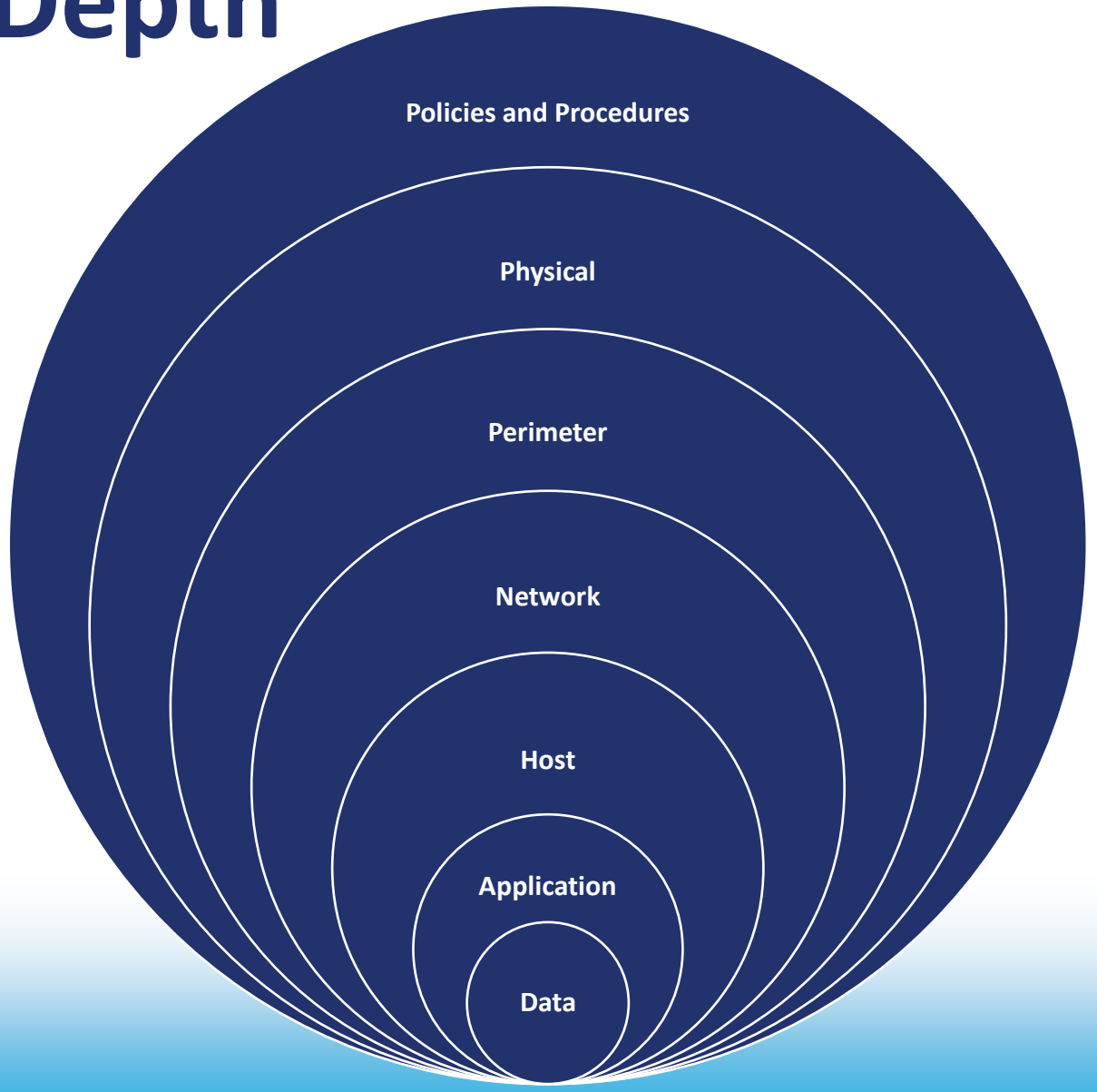
Administrative

- Policies
- Procedures
- Training
- BCP
- DRP
- IRP

Security Control Functions

- **Preventative**
  - Fences, locks
- **Detective**
  - Cameras, IDS, honeypots
- **Corrective**
  - Patching, reboot, restore

Defense in Depth



Compliance

Compliance involves adhering to rules, policies, standards, and laws set forth by industries and/or government agencies. Failing to do so could cost an organization in terms of poor performance, costly mistakes, fines, penalties, and lawsuits. - IBM

Compliance

- Following rules, regulations, and industry standards to meet legal, ethical, and operational requirements
- Involves meeting specific benchmarks or certifications and maintaining evidence and artifacts to prove adherence
- Requirements may vary depending on the sector, location, and organizational activities
- Goal is to avoid legal and regulatory penalties, reputational damage, and loss of customer trust when noncompliant
- Often focuses on minimum required

Governance Risk and Compliance (GRC)

An organizational strategy for managing governance, risk management, and compliance with industry and government regulations. GRC also refers to an integrated suite of software capabilities for implementing and managing an enterprise GRC program. – IBM

Think of GRC as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements. - CIO

Governance

At its basic level, governance is the set of rules, policies, and processes that ensures corporate activities are aligned to support business goals. It encompasses ethics, resource management, accountability, and management controls. - IBM

Risk Management

Identifying, assessing, and controlling financial, legal, strategic, and **security** risks to an organization. To reduce risk, an organization needs to apply resources to minimize, monitor, and control the impact of negative events while maximizing positive events. - IBM

Compliance Frameworks

- NIST CSF
- NIST 800-171
- CMMC
- CIS Controls
- ISO 27001
- HIPAA
- SOX
- SOC
- PCI DSS
- HITRUST
- ITARS
- MITRE ATT&CK

Compliance Example

Access Control (AC)		22*						
Basic Security Requirements								
Control #	**Description**	**Status**	**Evidence Captured**	**Assessment Method**	**Value**	**Score**	**Reviewed By**	**V**
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Compliant	N	POAM	5	5		
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Compliant	N	POAM	5	5		
Derived Security Requirements								
Control #	**Description**	**Status**	**Evidence Captured**	**Assessment Method**	**Value**	**Score**	**Reviewed By**	**V**
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Compliant	N	POAM	1	1		
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Compliant	N	POAM	1	1		
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Compliant	N	POAM	3	3		
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	Compliant	N	POAM	1	1		
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Compliant	N	POAM	1	1		
3.1.8	Limit unsuccessful logon attempts.	Compliant	N	POAM	1	1		
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Non-Compliant	N	POAM	1	-1		
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Compliant	N	POAM	1	1		
3.1.11	Terminate (automatically) a user session after a defined condition.	Compliant	N	POAM	1	1		
3.1.12	Monitor and control remote access sessions.	Compliant	N	POAM	5	5		
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Compliant	N	POAM	5	5		
3.1.14	Route remote access via managed access control points.	Compliant	N	POAM	1	1		
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	Compliant	N	POAM	1	1		
3.1.16	Authorize wireless access prior to allowing such connections.	Non-Compliant	N	POAM	5	-5		
3.1.17	Protect wireless access using authentication and encryption.	Compliant	N	POAM	5	5		
3.1.18	Control connection of mobile devices.	Non-Compliant	N	POAM	3	-3		
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	Non-Compliant	N	POAM	1	1		
3.1.20*	Verify and control/limit connections to and use of external systems.	Compliant	N	POAM	1	1		
3.1.21	Limit use of portable storage devices on external systems.	Non-Compliant	N	POAM	1	-1		
3.1.22*	Control CUI posted or processed on publicly accessible systems.	Non-Compliant	N	POAM	1	-1		
	Total Controls:	**22***	**0**	**SPRS**	**50**	**28**		

PCI DSS

Payment Card Industry Data Security Standard is set of security requirements designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment

- Created by the Payment Card Industry Security Standards Council (PCI SSC) comprised of the major credit card companies
- Mandatory for all merchants and service providers that process credit card transactions. Failure to comply with the standard can result in fines and other penalties
- Businesses fall into four groups. Larger businesses generally have more requirements
- 12 high-level requirements vary by business size and card transactions per year
- Complete a yearly assessment: most small businesses can perform a self-assessment
- Scan the network used to process payments. Requires the help of an outside firm
- Payment service providers (PSPs) like Square or Stripe can take on some compliance responsibilities making it easier to comply

ISO 27001

International standard for information security management system (ISMS). A framework for organizations to manage and protect their sensitive information, assets, and systems.

- Two parts:
  - Eleven Clauses (0-10)
    - Clauses 0 to 3 provide an introduction
    - Clauses 4-10 outline minimal compliance expectations for certification
  - Annex A - Defines 93 controls in four sections
- Requires all controls to be implemented listed in a “Statement of Applicability”
- Certification requires an independent audit by a 3rd-party certification body to verify that an organization's ISMS meets the requirements of the standard

NIST CSF

Guidelines, standards, and best practices for managing and reducing cybersecurity risk.

Compliance entails:

- Identify: systems, assets, data, and personnel that need to be protected, and conduct a risk assessment to identify and prioritize cybersecurity risks.
- Protect: Implement security controls to protect systems, assets, and data from unauthorized access, modification, or destruction.
- Detect: Implement security controls to detect cybersecurity incidents in a timely manner.
- Respond: Develop and implement an incident response plan to respond to cybersecurity incidents in a timely and effective manner..
- Recover: Develop and implement a plan to restore systems, assets, and data after a cybersecurity incident.
- Self Assessment

NIST SP 800-171

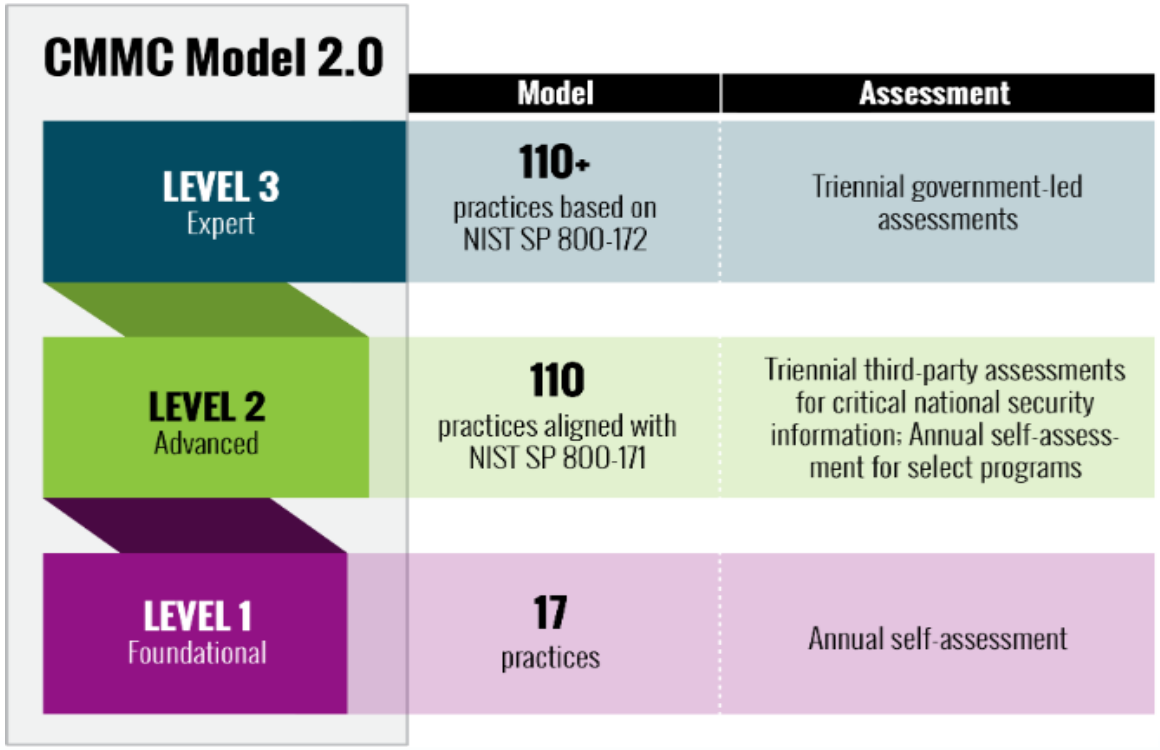
Defines security requirements for non-federal organizations (NFOs) that process, store, or transmit Controlled Unclassified Information (CUI) on behalf of the US government

- 14 control families derived from NIST 800-53
- 110 security requirements across the 14 NIST 800-171 families
- The requirements are categorized as either "basic" or "derived."
  - Basic requirements directly address the security objectives
  - Derived requirements are additional requirements that are necessary to achieve the security objective
- The requirements are non-prescriptive
- Each requirement has a discussion section that helps explain it
- Body of Evidence (BoE) contains deliverables:
  - System Security Plan (SSP)
  - Plan of Action and Milestones (POAM)
- Self Assessment

CMMC

Cybersecurity Maturity Model Certification (CMMC) is a framework developed by DoD that assesses and certifies the cybersecurity maturity of DoD contractors and subcontractors

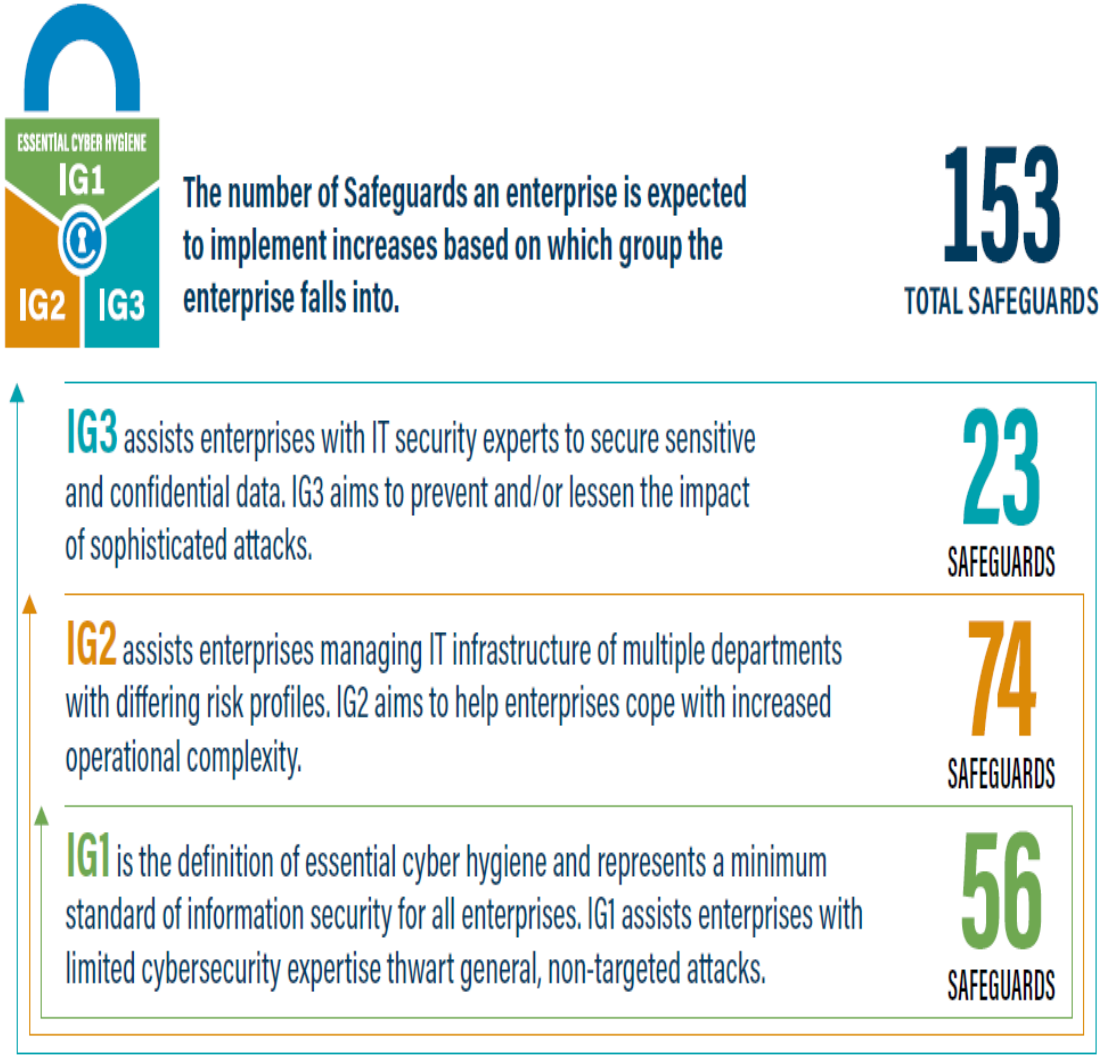
- Reduce the exfiltration of CUI
- Prompted by data breaches:
  - Impacting national security
  - Originating with NFOs
- Version 2.0 published in November 2021
- Based largely on NIST 800-171
- Achieve a level for an entire enterprise or particular segment(s) or enclave(s)
- Contracts containing DFARS 252.204-7012 must have at least a current Basic Assessment against NIST 800-171 in order to receive a contract award after 11/30/2020
- By 2025, DoD will require ALL defense contractors to pass a CMMC audit to bid on jobs



CIS Controls

The Center for Internet Security (CIS) Controls are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture

- Version 8
- 18 Control families
- 153 total safeguards
- Clear and easy to understand
- Easy to explain
- Maps to many other frameworks



CIS Controls

Frameworks Provided with CIS Controls Mapping

Australian Signals Directorate Essential Eight	FFIEC-CAT	NERC-CIP	SOC 2
Azure Security Benchmark v3	GSMA FS 31 Baseline Security Controls	New Zealand Information Security Manual v3.5	TSA Security Defense Directive Pipeline
CISA Cybersecurity Performance Goals (CPGs)	HIPAA	NYS Department of Financial Services 23 NYCRR Part 500	UK Cyber Essentials
CMMC	ISACA COBIT 19	NIST CSF	UK National Cyber Security Centre (NCSC) Cyber Assessment v3.1
Criminal Justice Information Services (CJIS)	ISO 27001:2022	NIST SP 800-53 R5	
CSA Cloud Controls Matrix v4	ISO/IEC 27002:2022	NIST SP 800-171	
Cyber Risk Institute (CRI) Profile v1.2	MITRE ATT&CK v8.2	PCI DSS	

Control Objectives

- Goals or outcomes that security controls aim to achieve in order to reduce risk and protect assets
- Based on an organization's security policy, risk assessment, and compliance requirements
- These should come BEFORE controls

Developing Control Objectives

- Identify and assess potential risks
- Determine likelihood and potential impact of each identified risk
- Prioritize risks based on likelihood and impact
- Develop control objectives that address identified risks
- Develop a plan to implement security controls to achieve control objectives

Control Objectives Example

Confidentiality:

- Ensure that only authorized users can access sensitive or confidential information
- Prevent unauthorized disclosure of sensitive or confidential information
- Protect sensitive or confidential information from unauthorized modification

Control Objectives Example

NIST 800-171 Requirement 3.4.1:

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

3.4.1 **Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.**

DISCUSSION

Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

[SP 800-128] provides guidance on security-focused configuration management.

Control Objectives Example

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

3.4.1 Establish and maintain baseline configurations and inventories of organization information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Are baseline configurations developed, documented, and maintained for each information system type?

Yes No Partially Does Not Apply Alternative Approach

Do baseline configurations include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations updated as needed to accommodate security risks or software changes?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations developed and approved in conjunction with the Chief Information Security Officer (CISO) or equivalent and the information system owner?

Yes No Partially Does Not Apply Alternative Approach

Are deviations from baseline configurations documented?

Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of company information systems. To apply the required security requirements within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. Security engineering cannot be properly applied if individuals who design, code, and test information systems and system components (including information technology products) do not understand security. It is important that developers include individuals on the development team who possess security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the company's business processes. This process also enables the integration of the information security architecture into the enterprise architecture, consistent with company risk management and information security strategies.

Where to Look:

- configuration management policy
- procedures addressing the baseline configuration of the information system
- procedures addressing configuration settings for the information system
- configuration management plan
- security plan
- enterprise architecture documentation
- security configuration checklists
- evidence supporting approved deviations from established configuration settings
- change control records
- information system audit records
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- change control records
- other relevant documents or records

Who to Talk to:

- employees with configuration management responsibilities
- employees with security configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

Control Objectives Example

CIS Controls To NIST 800-171 Mappings

CIS Control	CIS Sub-Control	Title	Description	Relationship	Req Type	171 Req Number	Requirement Description
1	1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	small subset	Basic	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
				small subset	Basic	3.5.1	Identify system users, processes acting on behalf of users, and devices.
1	1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	large subset	Basic	3.5.1	Identify system users, processes acting on behalf of users, and devices.
1	1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	large superset	Enhanced	3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.
1	1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	small subset	Basic	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
				small subset	Derived	3.1.16	Authorize wireless access prior to allowing such connections.
1	1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	Basic	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
				small subset	Derived	3.1.16	Authorize wireless access prior to allowing such connections.

Risk Management

- Process of identifying, assessing, and prioritizing potential risks to an organization's assets
- Taking steps to mitigate or manage those risks
- **A primary goal is to define control objectives**
- Example:

  A risk assessment identifies a potential risk of data breaches due to weak passwords; a control objective might be to require strong passwords and implement password complexity requirements for all users.

Risk Assessment

- Systematic process to identify, analyze, and prioritize risks
- Key elements:
  - asset identification
  - threat analysis
  - vulnerability assessment
  - risk evaluation
- Benefits:
  - Strengthen security posture
  - Improve / maintain compliance
- Evolving threat landscape requires regular review and updates to the risk assessment

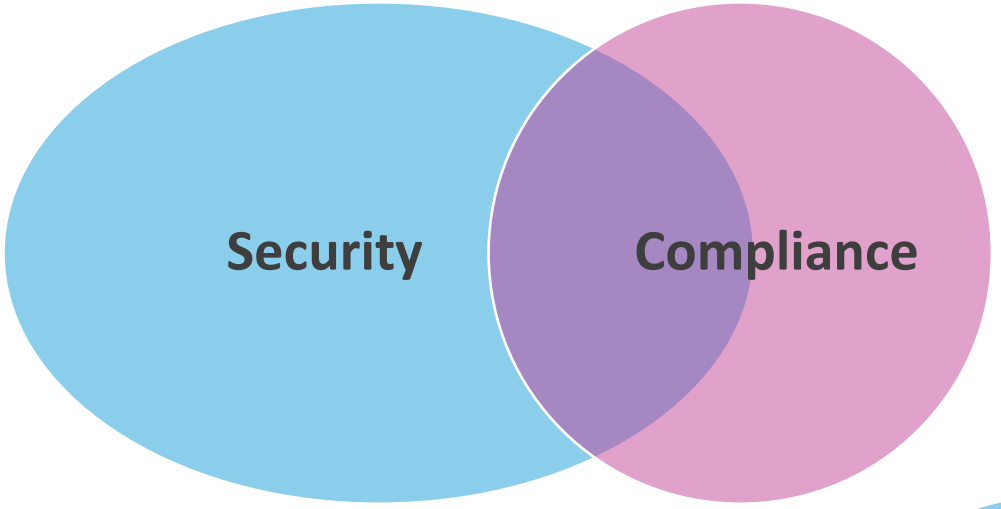
GRC Tools

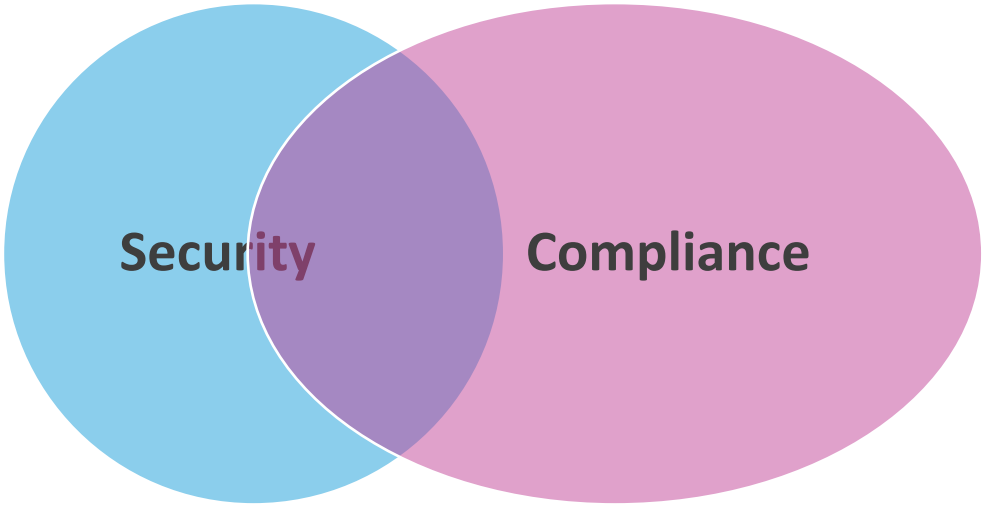
- Cover risk, compliance, IT governance, and internal auditing
- Ensure organization is meeting compliance and risk standards
- Map controls to regulations and compliance requirements

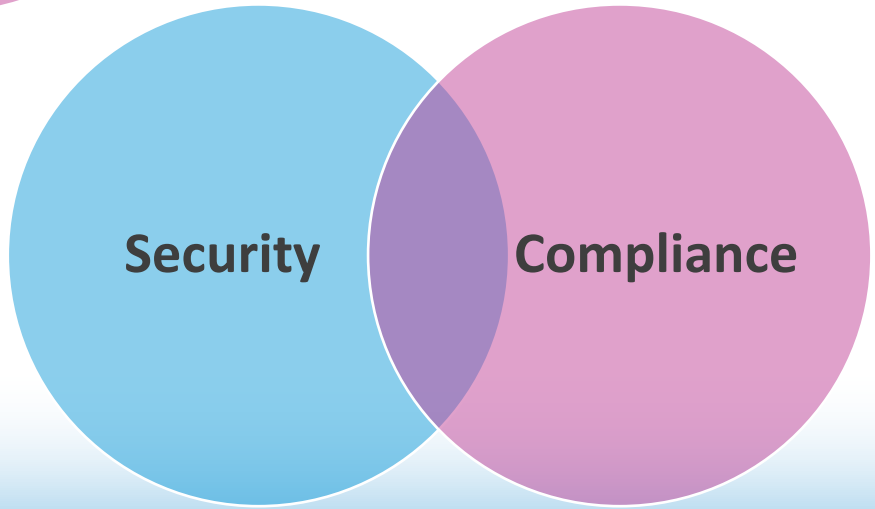
GRC Tools

- ServiceNow GRC
- IBM OpenPages
- LogicManager
- SAI360
- Riskonnect
- SolarWinds Security Event Manager
- Netwrix Auditor
- StandardFusion

Security vs Compliance





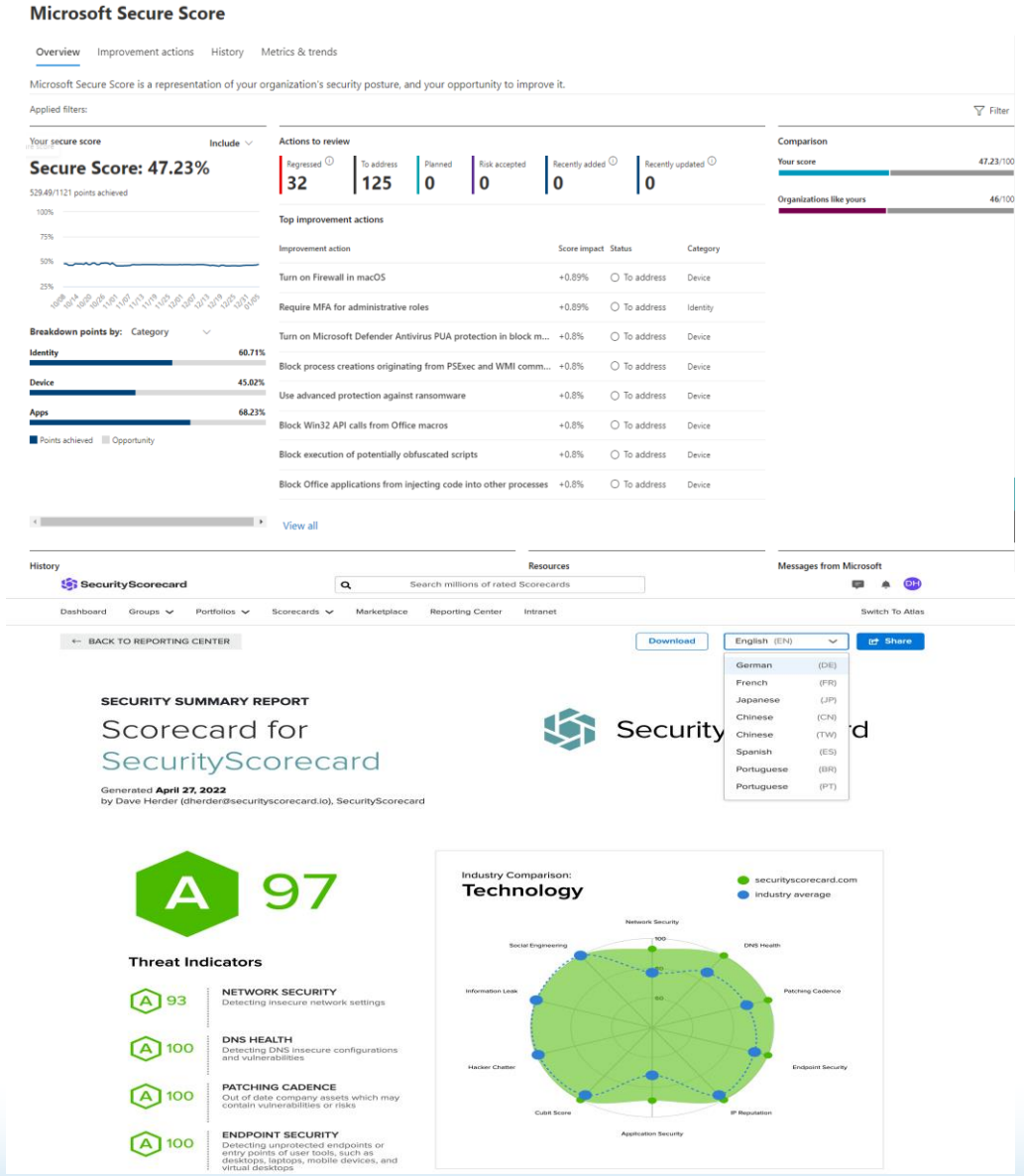


Strategy

- Understand organizational risk appetite
- Take a risk-based approach
- Perform a risk assessment
- Determine the need and/or value of compliance
  - **It can be a heavy lift to achieve full compliance with most frameworks**
  - Compliance can be a competitive advantage
  - Ensure you start with current version
  - Limit scope when possible
  - CIS Controls is a great place to start
- Define control objectives

Strategy

- Select appropriate controls to meet control objectives
- Implement controls
- Monitor and report on controls
- Monitor and report on risk
- Leverage tools for monitoring and visibility
- Adjust accordingly
- Keep up with trends and compliance changes



Conclusion

- **Security**
  - Driven by need to protect
  - Done for its own sake
  - Requires continuous monitoring and improvement
  - A prerequisite for compliance
- **Compliance**
  - Driven by business needs
  - Done to satisfy external requirements
  - Provides accountability
  - Ends when 3rd-party is satisfied
  - Support security

Conclusion

- Security and compliance **can and should complement each other**
  - Compliance establishes a baseline
  - Compliance provides guidance and benchmarks
  - Security builds on the baseline based on risk tolerance and appetite
- Compliance can help identify security gaps
- Compliance can baseline security based on best practices
- **A focus on both:**
  - Allows organizations to improve their security posture AND demonstrate a strong commitment to security
  - May reduce insurance costs and provide competitive advantage

Conclusion per ChatGPT

Understanding the distinction between security and compliance is vital for cybersecurity professionals. While security focuses on protecting systems and data from threats, compliance ensures adherence to legal, regulatory, and industry-specific requirements. Both concepts are interdependent and must be addressed to build a comprehensive cybersecurity program. By implementing robust security measures, organizations can achieve compliance and demonstrate their commitment to safeguarding sensitive information.

Your chocolate's in my peanut butter! No your peanut butter is on my chocolate!

For more information…

- Bruce Schneier:@schneierblog
- Kevin Mitnick: @kevinmitnick
- US-CERT: @USCERT_gov
- SecurityWeek: @SecurityWeek
- Center for Internet Security: @CISecurity
- MSRC: @msftsecresponse
- NIST Cyber: @NISTcyber
- Intrust IT: @IntrustIT
- CISA: CISAgov
- MSRC: @msftsecresponse
- Microsoft Secure: @msftsecurity
- RSA: @RSAsecurity
- Mikko Hypponen: @mikko
- Troy Hunt: @troyhunt
- CSOnline: @CSOonline
- Me: @DaveHatter

Additional Resources

- https://www.nist.gov/cyberframework
- https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- https://www.iso.org/isoiec-27001-information-security.html
- https://dodcio.defense.gov/CMMC/
- https://www.pcisecuritystandards.org/
- https://www.cisecurity.org/controls
- https://www.cisecurity.org/insights/white-papers/cis-controls-and-sub-controls-mappings-to-nist-special-publication-800-171-r2
- https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security
- https://chat.openai.com/chat

Q & A

"You are an essential ingredient in our ongoing effort to reduce Security Risk."

- Kirsten Manthorne

Thank You!

Dave Hatter, CISSP, CISA, CISM, CCSP, CCSLP, Security +, Network+, PMP, ITIL

Intrust IT

linkedin.com/in/davehatter

twitter.com/davehatter

Get our checklist:
https://www.intrust-it.com/cyber-security/cyber-essentials-checklist/

Catch Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or
http://55krc.iheart.com

Catch Cyber Monday live on WTVG at 6:30 AM every Monday on 13 ABC or
https://www.13abc.com/

Don't forget to fill out your

SESSION SURVEY