THE POWER OF BEING UNDERSTOOD

Improving Cybersecurity Through Effective Assessments

With you today

Ron Ritenour, MBA, HCISPP, CISA

Manager, Security, Privacy and Risk Services

Ron has extensive experience in developing risk-based strategies, programs, policies and standards that align with business goals to support the expansion and transformation of business requirements. Frameworks include OCR HIPAA, NIST SP 800-x, NIST CSF, CIS CSC, ISO, OWASP and COBIT, focusing on information/IT security, people, process and technology. Ron has extensive experience in communicating information security strategies; making recommendations to senior management and Board members; and managing vendor performance to ensure service level requirements are achieved. Ron has experience serving as a HIPAA security officer, managing an information security department and serving as the chair of an information security council.

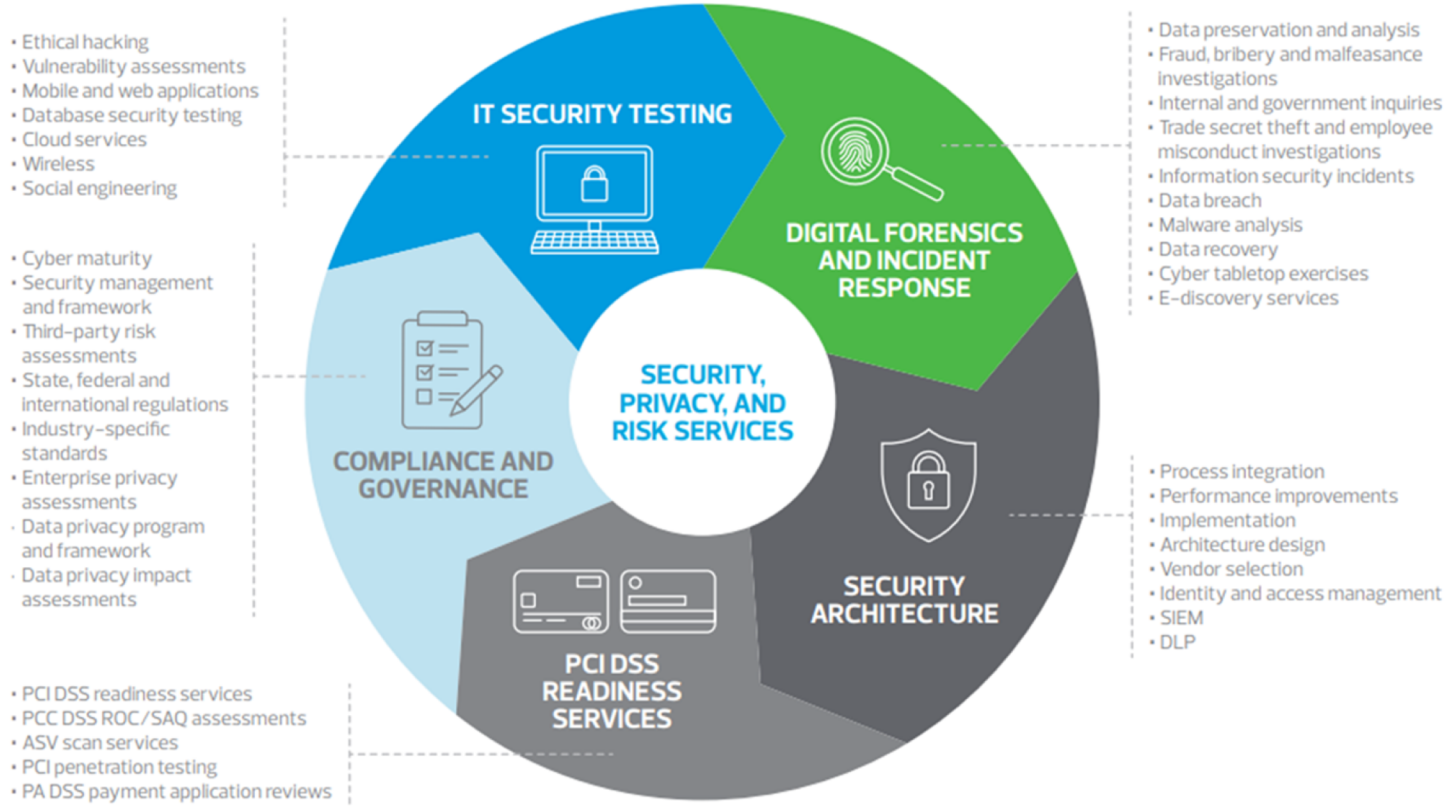
RSM overview

The power of being understood

- Fifth largest audit, tax and consulting firm in the United States
  - Over $1.9 billion in revenue
  - 85 cities and more than 10,000 employees in the United States
- U.S. member of the sixth largest independent network of audit, tax and consulting firms globally*
  - Presence in more than 120 countries
  - More than 43,000 people in over 800 offices
  - $5.1billion (U.S.) in worldwide revenues

* RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/about us for more information regarding RSM US LLP and RSM International.

Security, privacy and risk consulting overview



Improving Cybersecurity Through Effective Assessments

ASSESSING SECURITY

Risk Assessments

RSM

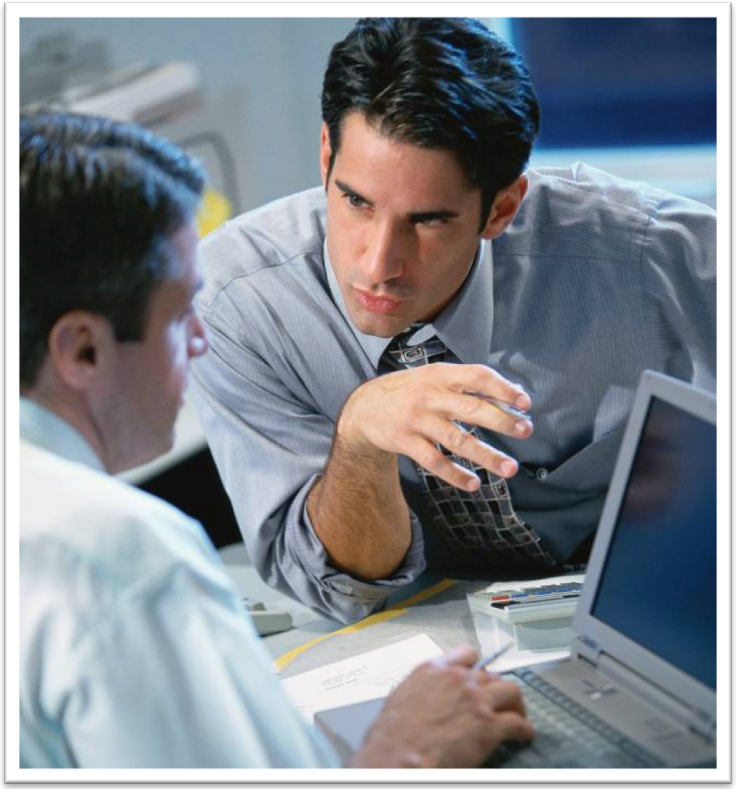
Why do a Security Assessment?

Assessments can help to measure, manage, and mitigate risks. How?

- Risk assessments
  - Identify what security risks exist in the environment and evaluate their impact to business operations, compliance posture, etc.
  - Provide important context into subsequent evaluations (even within the same project)
- Maturity assessments
  - Evaluate current maturity levels of security practices based on a given framework
  - Recommend target maturity levels based on the identified risk profile and business priorities
- Gap assessments
  - Identify tactical gaps between the current state and a desired target state (e.g. security maturity level, regulatory compliance, etc.)

Elements of Risk

- Elements of risk
  - Financial risk
  - Operational risk
  - Strategic risk
  - Regulatory/legal
  - Reputation
  - Others



RSM

Risk Management Stakeholders

- Information Systems Security
- IT and Operations Management
- System and network administration
- Internal Audit
- Physical Security
- Business Process and Information Owners
- Health, Safety, and Environmental
- Human Resources
- Legal

Aligning Security with Business Risk

- Risk assessment
  - A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures
  - The process of evaluating threats and vulnerabilities—known and postulated—to determine expected loss and establish the degree of acceptability to system operations

RSM

Risk Assessment Types

- Qualitative:
  - Evaluates risk objectively (high, medium, low)
  - Allows you to determine which areas need the most control
- Quantitative:
  - Evaluates risk in dollar figures
  - Requires that dollar amounts be assigned to assess possible but improbable events

RSM

Improving Cybersecurity Through Effective Assessments

ASSESSING SECURITY

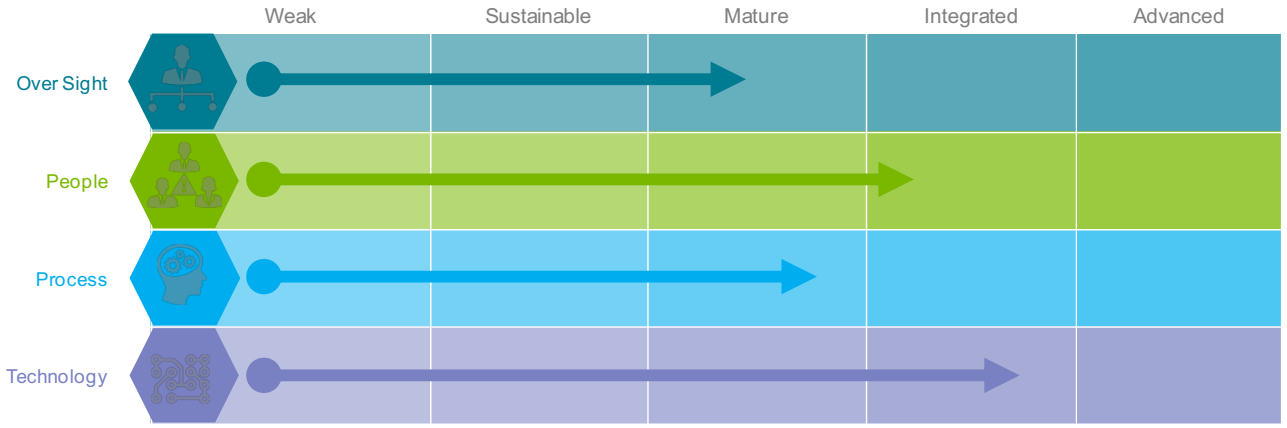
Maturity Assessments

RSM

Cyber Maturity continuum

Takeaways:

- Not all areas need to reach the same level of maturity, and rarely do companies need to extend beyond a “3” in maturity
- Target maturity should be decided as a balance of risk vs. cost



Weak	Sustainable	Mature	Integrated	Advanced
▪ Security governance pre-requisites for a formal security management framework are not in place. ▪ Security processes and frameworks are siloed, ▪ Undocumented & inconsistent processes ▪ Security activities are not aligned with business strategy. ▪ Security capabilities are dependent on individuals. ▪ Cyber risks are not consistently considered as business decisions are made.	▪ The business does the minimum to meet the expectations of internal and external stakeholders. ▪ Select security activities are defined; some of which are aligned with business strategy. ▪ Security capabilities vary across the “three lines of defense”. ▪ Limited and inconsistent use of supporting technology. Limited focus on emerging risks and/or scenario analysis.	▪ The board and executives are increasingly confident that security risks are being effectively managed based on emerging threats, external benchmarking, and the use of risk appetite, tolerances and limits. ▪ Risk Management activities are aligned with business strategy. Security management functions demonstrate a level of consistency, but remote operations or business entities are not integrated. Use of technology is not integrated.	▪ Security management capabilities and activities are integrated and coordinated across corporate and remote operations and business entities. ▪ Security management objectives and value proposition are consistently aligned with business strategy. ▪ Common tools and processes are used with enterprise-wide risk monitoring, measurement and reporting.	▪ Risk management activities are fully embedded in strategic planning, capital allocation, and in daily decision making. ▪ An early warning system is in place to notify the board and management of risks above established thresholds. ▪ Security management serves as a source of competitive advantage. ▪ Incentive compensation formally considers risk management.

RSM

Understand your risk (and cost) tolerance

Lower complexity
Lower risks

It's important to find the "sweet spot" for your organization's security target:

- Enterprise risk assessments
- Technology / process portfolio analysis
- Security threat analysis
- Executive leadership signoff of:
  - ✓ IT strategy
  - ✓ Risk acceptance

Higher complexity
Higher risks

RSM

Improving Cybersecurity Through Effective Assessments

SECURITY GOVERNANCE – REGULATIONS AND FRAMEWORKS

RSM

Security Regulations vs. Frameworks

Regulatory Sources:

- **FFIEC IT Handbook** – IT operations and security requirements for financial institutions
- **PCI DSS** – Security requirements for organizations handling credit card information / transactions
- **GDPR** – Data privacy requirements affecting companies storing or processing the personal data of anyone within the European Union
- **State Privacy Laws (e.g. CCPA)** – each state has its own privacy laws with varying levels of requirements for basic privacy rights, breach notification, etc.

Security Frameworks:

- **FFIEC CAT / FSSCC ACAT** – Risk profile and security maturity evaluation tool
- **NIST CSF** – Simplified security framework with mapping to multiple regulations / frameworks
- **FSSCC Cybersecurity Profile** – Tailored version of NIST CSF for Financial Services. CAT 2.0?

FFIEC CAT – Inherent Risk Profile

INHERENT RISK PROFILE

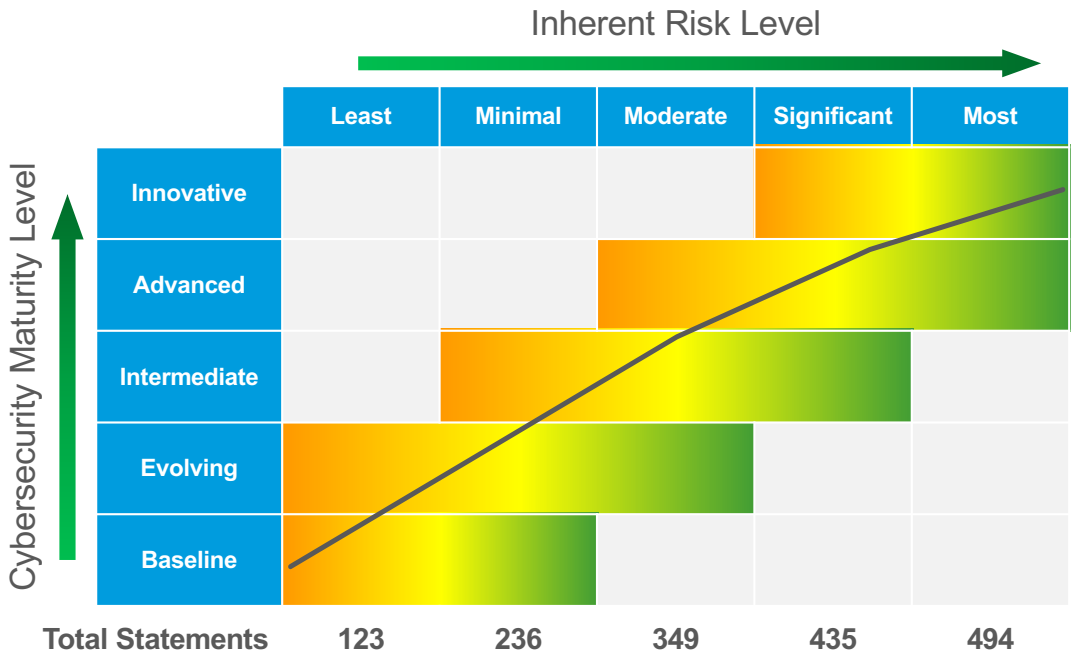
Technologies and Connection Types	Risk Level									
	Least		Minimal		Moderate		Significant		Most	
Total number of internet service provider (ISP) connections (including branch connections)	N	No connections	Y	Minimal complexity (1–20 connections)	N	Moderate complexity (21–100 connections)	N	Significant complexity (101–200 connections)	N	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., File Transfer Protocol [FTP], Telnet, rlogin)	Y	None	N	Few instances of unsecured connections (1–5)	N	Several instances of unsecured connections (6–10)	N	Significant instances of unsecured connections (11–25)	N	Substantial instances of unsecured connections (>25)
Wireless network access	N	No wireless access	Y	Separate access points for guest wireless and corporate wireless	N	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	N	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	N	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	Y	None	N	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	N	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	N	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	N	types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some ap accesse
Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., Virtual Private Network, modem, intranet, direct connection)	N	No third parties and no individuals from third parties with access to systems	Y	Limited number of third parties (1–5) and limited number of individuals from third parties (<50) with access; low complexity in how they access systems	N	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems	N	Significant number of third parties (11–25) and significant number of individuals from third parties (501–1,500) with access; high level of complexity in terms of how they access systems	N	Any dev availabl employ executi and boa applicat

FFIEC CAT uses a parameter-based spreadsheet with 39 technology risk areas to clearly score a bank's inherent risk level.

Banks should be able to do this themselves, but we are often asked to perform it or at least validate their results

Category	Total Statements	Average Risk Score	Inherent Risk Level
Technologies and Connection Types	14	1.57	Minimal
Delivery Channels	3	4.33	Significant
Online/Mobile Products and Technology Services	14	1.64	Minimal
Organizational Characteristics	7	2.14	Minimal
External Threats	1	2.00	Minimal
Overall	39	2.34	Minimal

FFIEC CAT - Cybersecurity Maturity Assessment



- Risk level determined in the Inherent Risk Profile dictates the appropriate maturity level
- Banks may reside anywhere in the continuum for their risk level…but examiners want most banks to aim for at least “Evolving”

FFIEC CAT - Output

Inherent Risk Profile

Category	Total Statements	Average Risk Score	Inherent Risk Level
Technologies and Connection Types	14	1.57	Minimal
Delivery Channels	3	4.33	Significant
Online/Mobile Products and Technology Services	14	1.64	Minimal

Cybersecurity Maturity

Assessment Factor	Area /Maturity	Baseline	Evolving
Domain 1: Cyber Risk Management Oversight			
Governance	Oversight	80%	25%
	Strategies/Policies	57%	0%
	IT Asset Management	25%	50%
Risk Management	Risk Management Program	100%	67%
	Risk Assessment	67%	0%

Domain 1: Cyber Risk Management Oversight

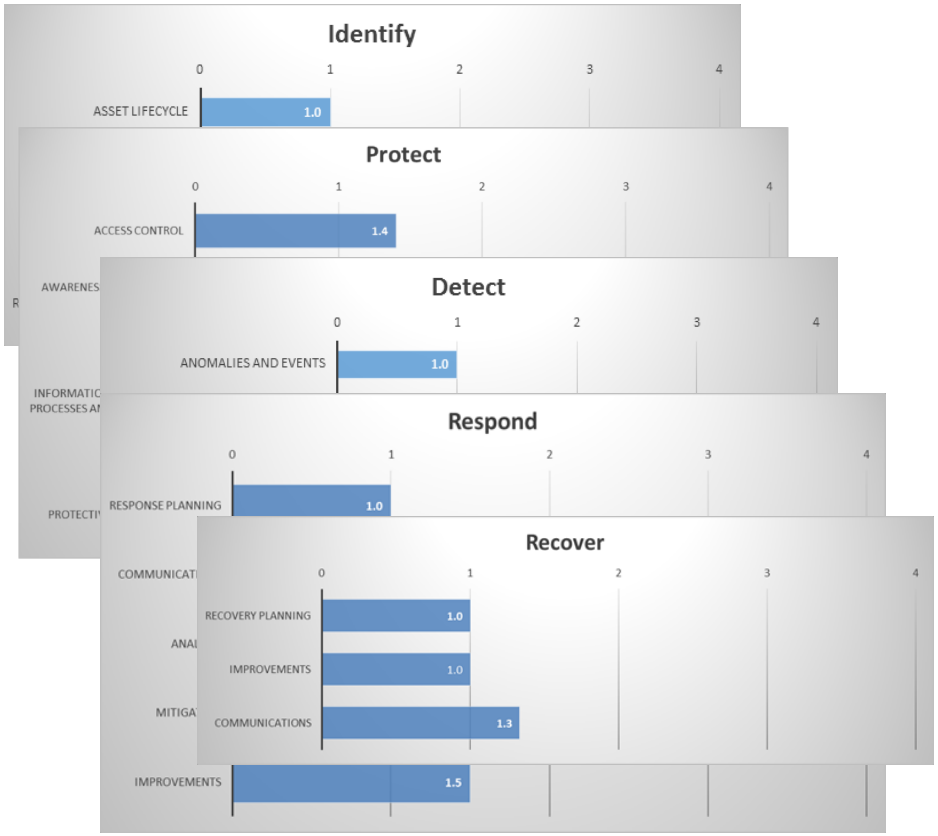
Assessment Factor	Area	Maturity	#	Y/N	FFIEC Question
	Oversight	Baseline	1	Y	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, Page 3)
			2	Y	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, Page 6)
			3	N	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, Page 5)
			4	Y	The budgeting process includes information security-related expenses and tools. (FFIEC E-Banking Booklet, Page 20)
			5	Y	Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, Page J-12)

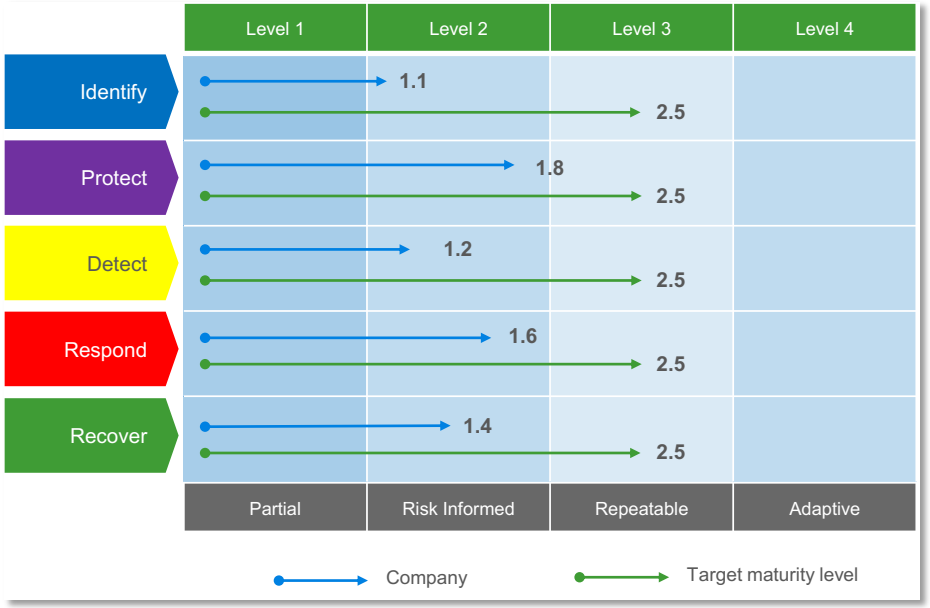
NIST Cybersecurity Framework

NIST Cybersecurity Framework v1.1				
Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management, Authentication and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

RSM

NIST CSF and Cyber maturity





Improving Cybersecurity Through Effective Assessments

BUILDING SECURITY CONTROL FRAMEWORKS

Security Framework Development

Security Standards / Regulations

ISO

NIST National Institute of Standards and Technology U.S. Department of Commerce

DFARS

PCI Security Standards Council

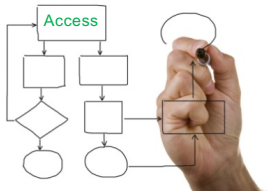
IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SANS 20 CRITICAL SECURITY CONTROLS

HITRUST Health Information Trust Alliance

Common Objectives



Control Mapping

Over Sight	People	Process	Technology
Understanding of Cyber Threats	Security Awareness & Training	Identity & Access Management	Security Architecture & Design
Board & Executive Oversight	Organizational Culture	Incident Management	Security Monitoring
Security Governance & Strategy	Communications	Vulnerability & Malware Management	Threat Modelling
Regulatory & Legislative Compliance	Security Organization Structure	Sourcing & Vendor Management	Intrusion Detection & Prevention
Public Relations	Roles & Responsibilities	Information Asset Management	Configuration Management
Cyber Insurance	Security Skills & Competency	Application & System Development	End Point Security
Litigation & Investigation		Business Continuity	Data Loss Prevention
Coordination with Law Enforcement		Physical Security	
Effective Management of Cyber Risk			

RSM

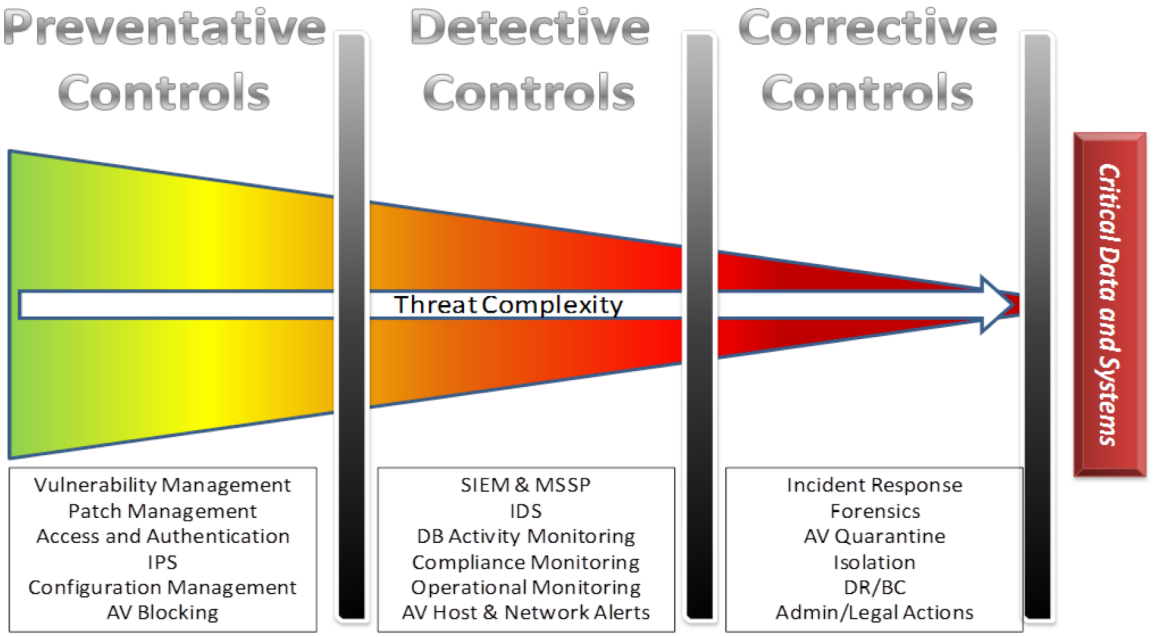
Control Types

- Preventative—System rules that do not allow a user to affect the CIA of information (e.g., access controls, firewalls)
- Detective—Systems or methodologies that inform management a breach of security has occurred (e.g., intrusion detection system [IDS], audit trail)
- Corrective—Used to mitigate risks from unlikely or catastrophic violations of the system's security (e.g., CIRT, insurance, backup tapes)
- A core concept of 'Defense in Depth'

RSM

Defense in Depth

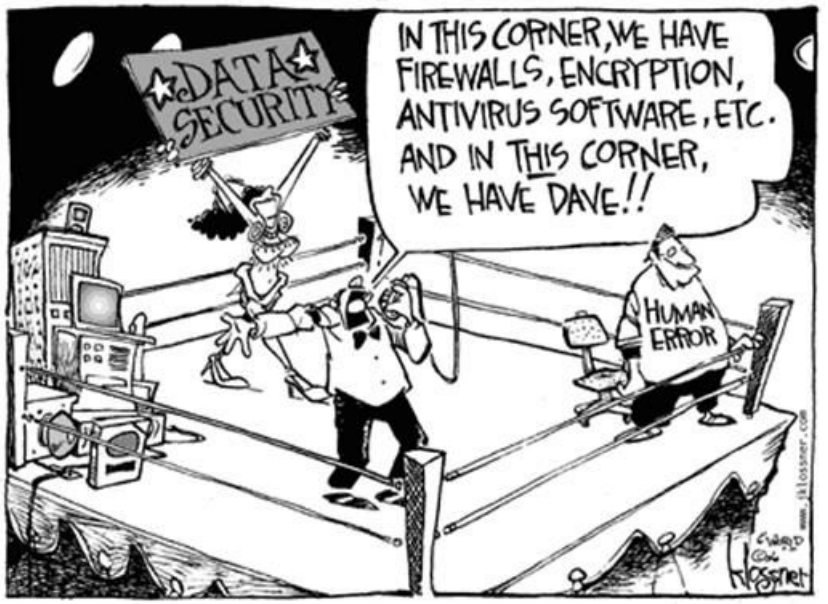
- Understand that modern threats are built to bypass preventative controls.
- Adjust your audit focus to detective and corrective controls.



RSM

Defense in Depth: People

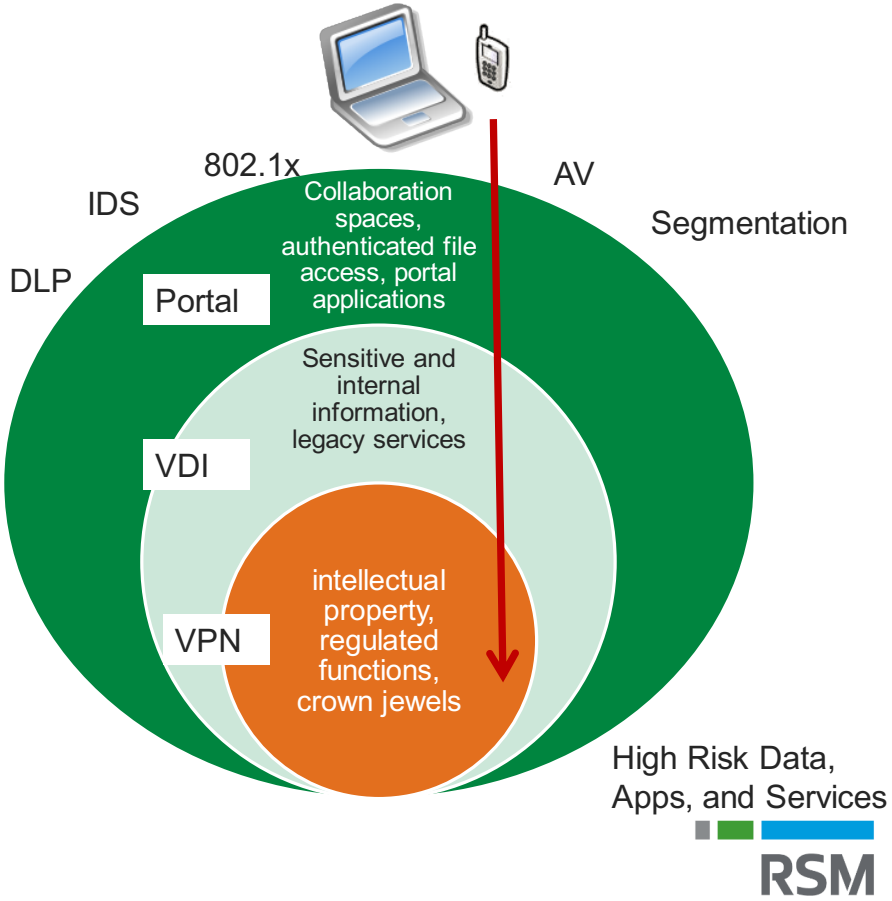
- Help and strengthen (but don't bash) the most vulnerable part of the network!
- Comprehensive security training program
  - Both general security best practices and social engineering
- Physical security of assets
  - Monitor who has access, as well as when they use their access
- User account administration / appropriate permissions
  - Why is it a bad idea for everyone to have local administrative rights?



Defense in Depth: Technology

Establish layers of technical protections defend against, detect, and contain attacks:

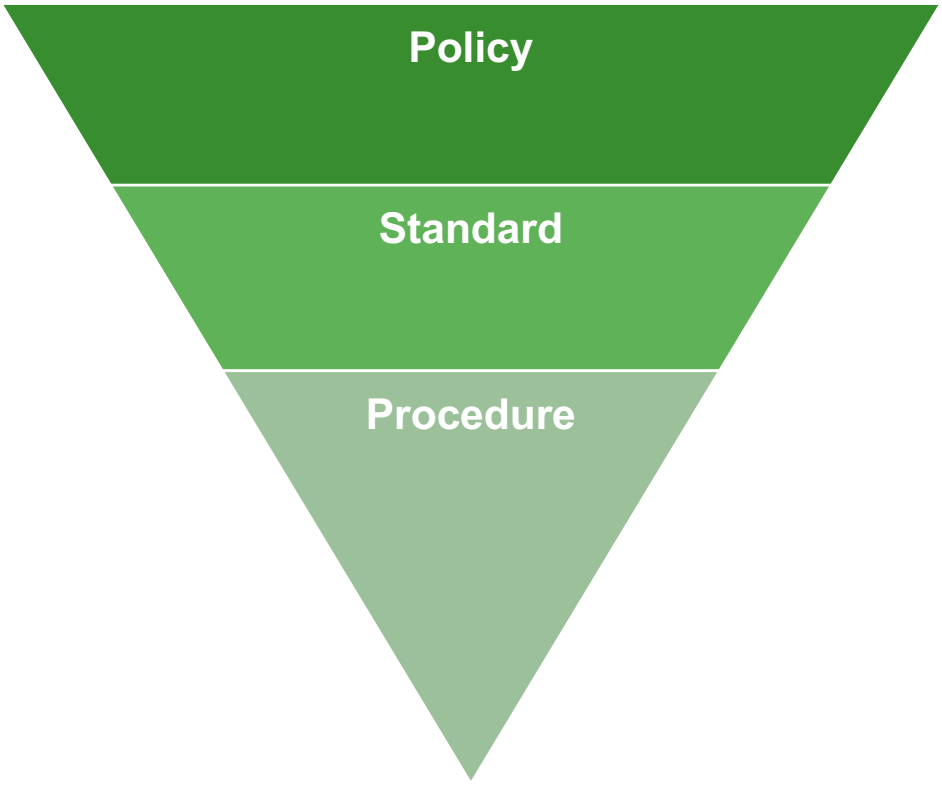
- Network segmentation
- Intrusion prevention/detection systems (IPS/IDS)
- Patching
- Anti-malware software
- System hardening
- Data loss protection (DLP) tools
- Logging and monitoring



Improving Cybersecurity Through Effective Assessments

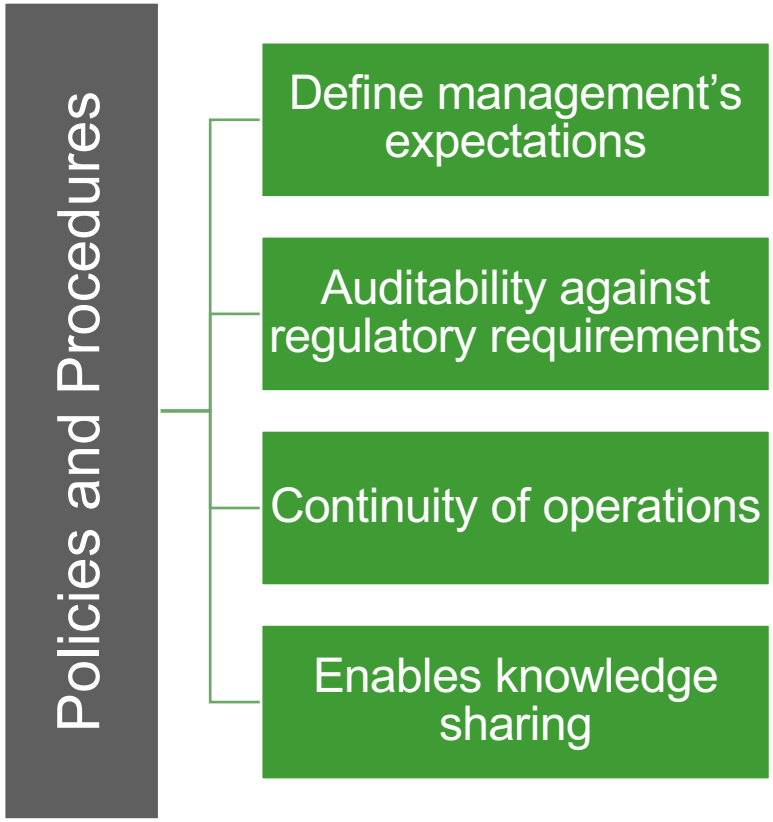
INFORMATION SECURITY POLICIES AND PROCEDURES

- Policies, procedures, and standards – what's the difference?
- Policy
  - The "why" – policies outline goals for what should be done and who is responsible, but don't dictate how to accomplish the stated goals
- Standard
  - The "what" – standards are tactical documents that lay out the specifics required to meet a certain requirement
- Procedure
  - **The "how"** – procedures are step-by-step documents that detail exactly how policies and standards are to be met



RSM

Why is Documentation Important?



"Man cannot live by institutional knowledge alone"

Having effective processes and knowledgeable team members is important, but it isn't everything:

- Policies clearly set expectations for team members to follow
- Auditable compliance usually requires formal documentation of processes
- Reliance on institutional knowledge can slow knowledge transfer and continue the "brain drain" issue facing many companies

RSM

What Security Policies Should I Have?

Depends on what your control framework and compliance obligations are. Policies should first be designed to align with those.

Many security frameworks include topic areas that would require supporting policy elements such as:

Asset Management	Incident Response
Access Management	Business Continuity / Disaster Recovery
Change / Configuration Management	Personnel Security
Patch / Vulnerability Management	Third Party / Vendor Management
Logging and Monitoring	Data Classification / Retention
Risk Management	

RSM

QUESTIONS AND ANSWERS