Lessons Learned From A 2 Year Old Cat

NEARLY 1200 FINANCIAL INSTITUTIONS HAVE COMPLETED SBS' CYBER-RISK TOOL; WHAT CAN WE LEARN?

PRESENTED BY:
JON WALDMAN, PARTNER – SBS – CISA, CRISC

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Contact Information

- Jon Waldman
  - Partner, EVP IS Consulting
  - CISA, CRISC
  - Master's of Information Assurance, Dakota State University
  - Mission: save the world!
  - Phone: 605-380-8897
  - jon@sbscyber.com
  - www.sbscyber.com
- SBS Institute
  - sbsinstitute@sbscyber.com
  - 605-269-0909

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

FFIEC “CAT” Overview

FFIEC Cybersecurity Assessment Tool **User’s Guide**

User’s Guide

Overview

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council[1] (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity maturity.

https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Risk Management Approach

- Tier 1 FFIEC CAT = Organizational Risk Assessment
  - Cyber-Risk: https://cyber-risk.protectmybank.com/
- Tier 3 TRAC = Asset Based Risk Assessment
  - TRAC: https://sbscyber.com/products/trac

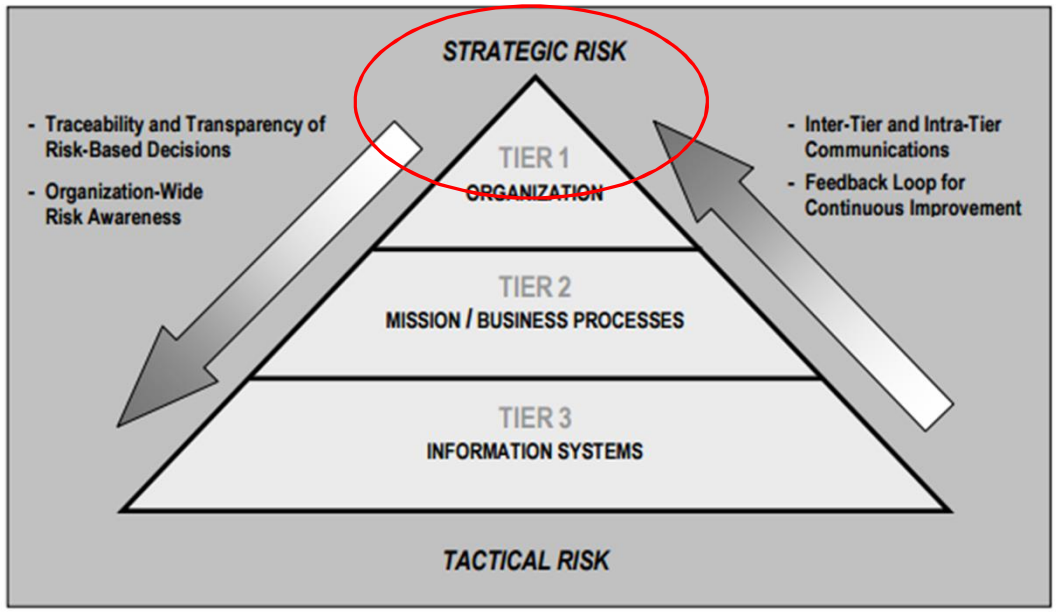
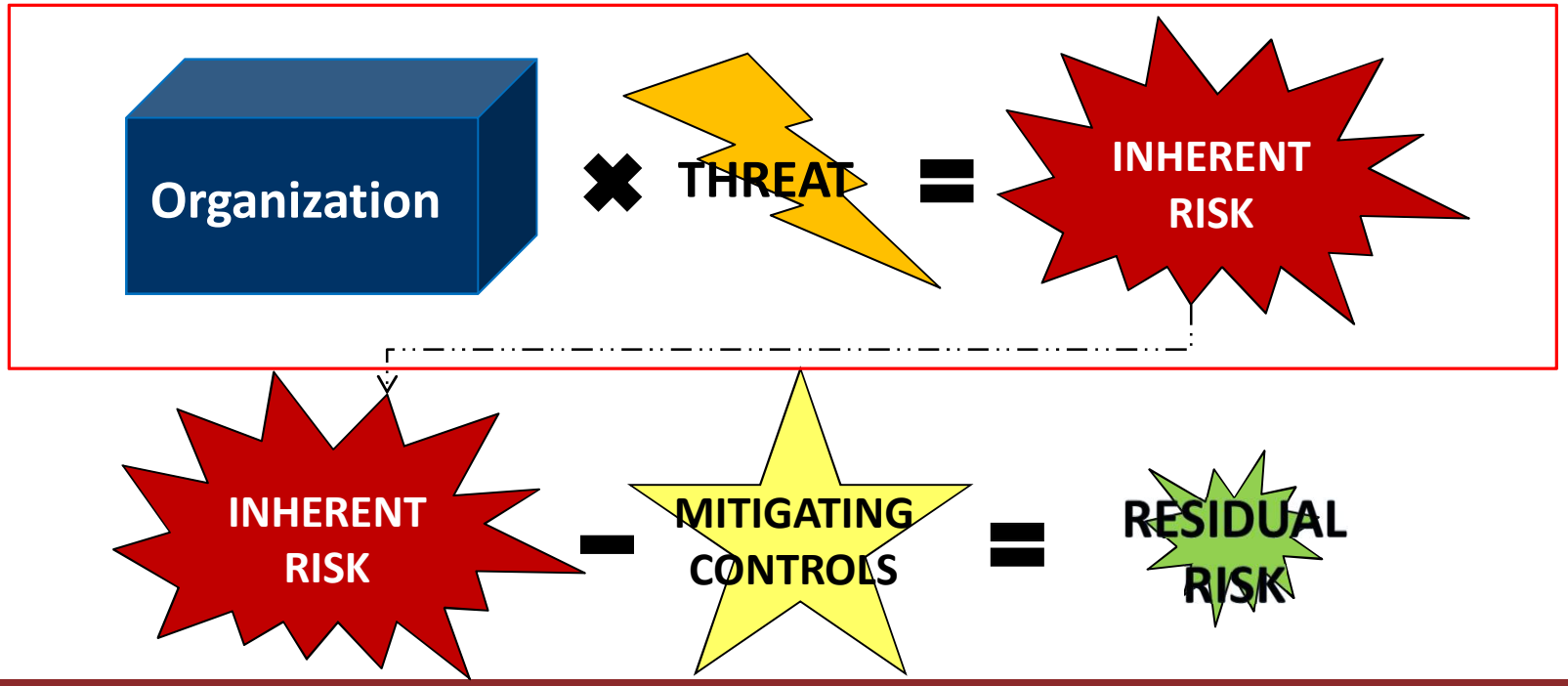


FIGURE 4: RISK MANAGEMENT HIERARCHY

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Risk Assessment Formula

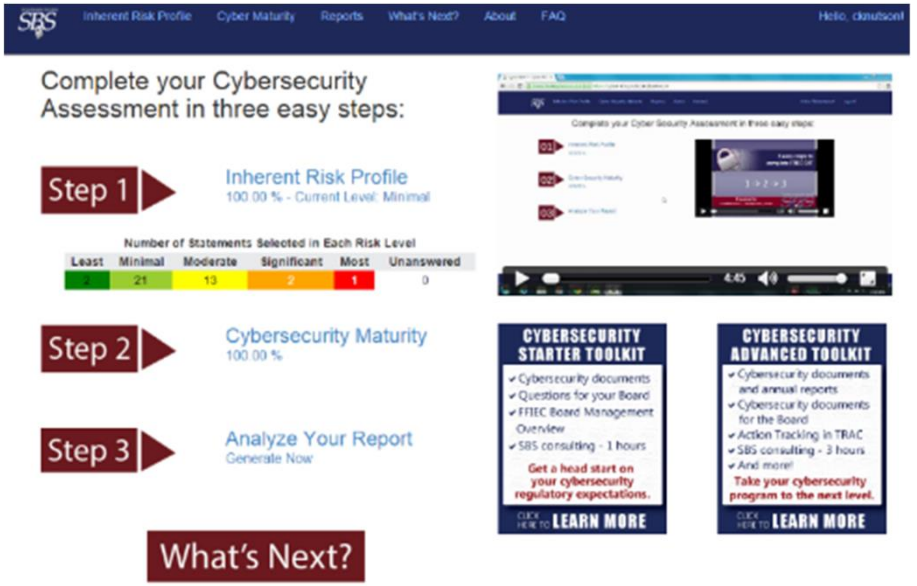
- Based on NIST 800-30
- FFIEC simplified approach, concept same.
- Focus on first part of process.



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

SBS Cyber-RISK

- Web based FFIEC Cybersecurity Assessment Tool
  - www.sbscyber.com
- Complimentary Access
- Over 1300 active users
- Nearly 1200 completed assessments
- 100% Follows FFIEC CAT



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

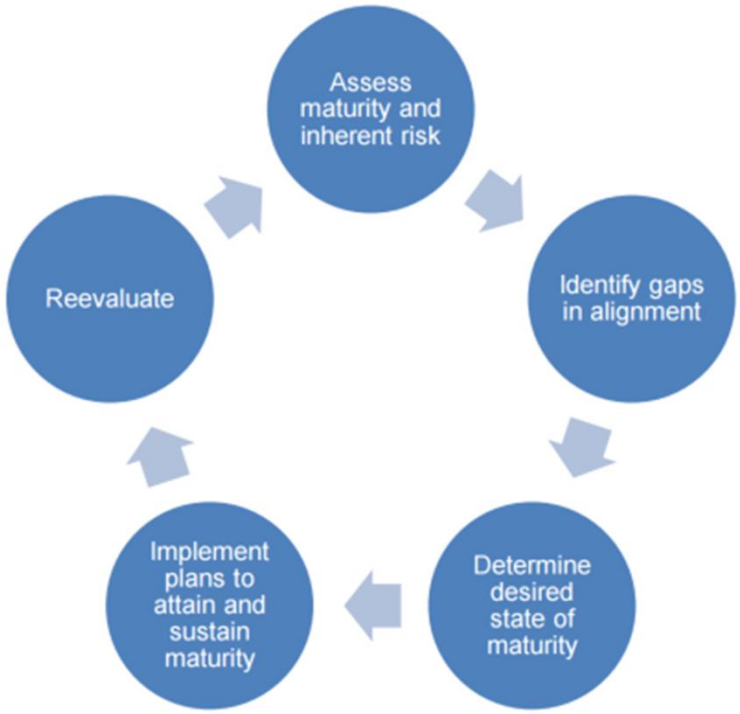
FFIEC CA Tool (3 parts)

- Three (3) major components
  1. Rating your **Inherent Risk** for Cybersecurity threats based on your size and complexity
  2. Rating your **Cybersecurity Maturity** regarding how prepared you are to handle different Cybersecurity threats
  3. **Interpreting and analyzing** your results by understanding how your Inherent Risk ties to your Cybersecurity Maturity, and where you SHOULD be regarding risk vs. maturity.

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

FFIEC CAT Process

1. Determine Inherent Risk
2. Determine Domain Maturity
3. Identify Goals
4. Identify Gaps
5. Implement additional controls
6. Increase maturity
7. Repeat



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Cybersecurity Inherent Risk

Å Five Inherent Risk Areas (39 Questions)

1. Technologies and Connection Types
2. Delivery Channels
3. Online/Mobile Products and Technology Services
4. Organizational Characteristics
5. External Threats

Least Inherent Risk → Minimal Inherent Risk → Moderate Inherent Risk → Significant Inherent Risk → Most Inherent Risk

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

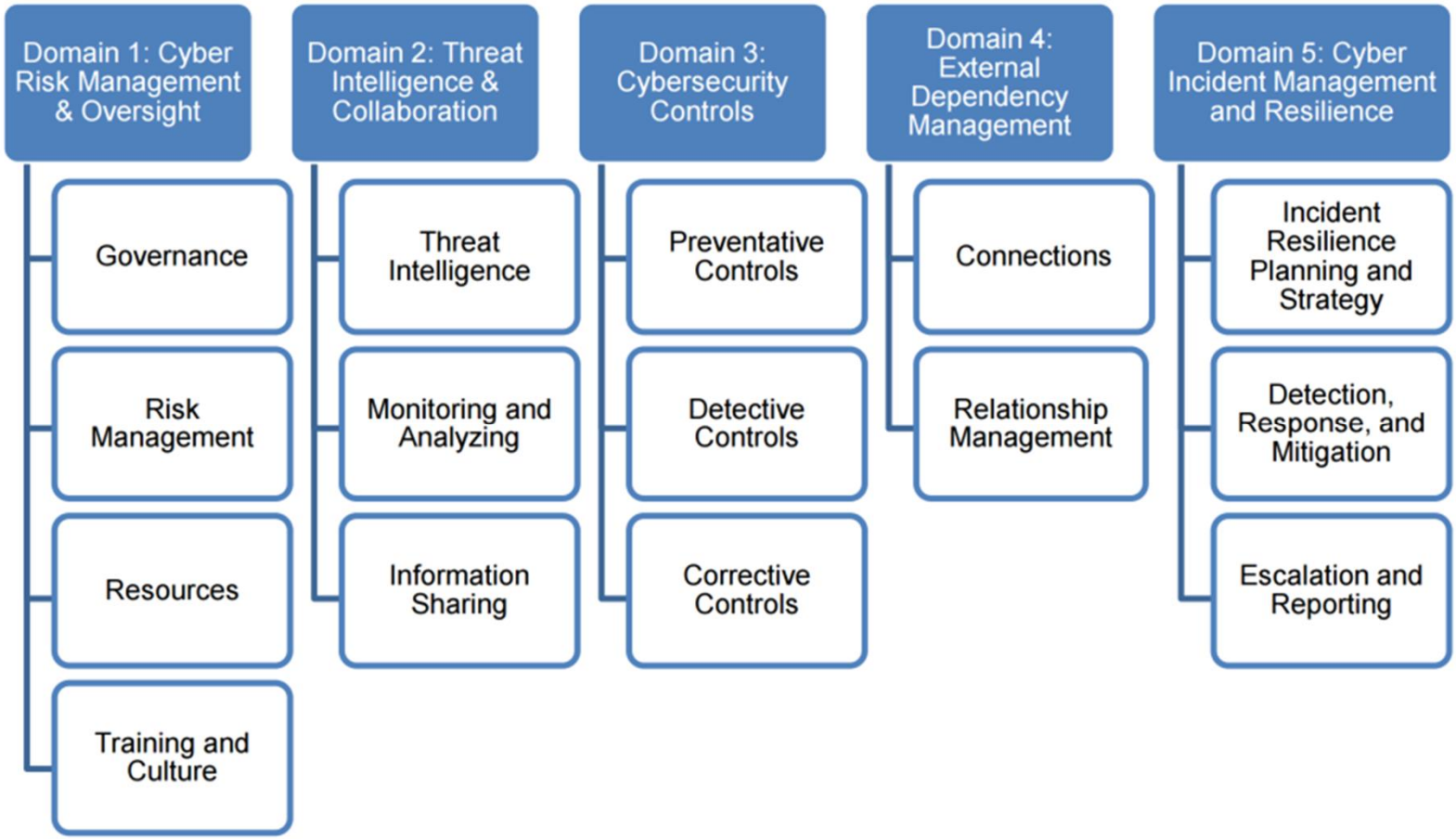
Inherent Risk Profile

Inherent Risk Profile

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	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	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed
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)	No third parties and no individuals from third parties with access to systems	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	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	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	Substantial number of third parties (>25) and substantial number of individuals from third parties (>1,500) with access; high complexity in how they access systems

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Cybersecurity Maturity

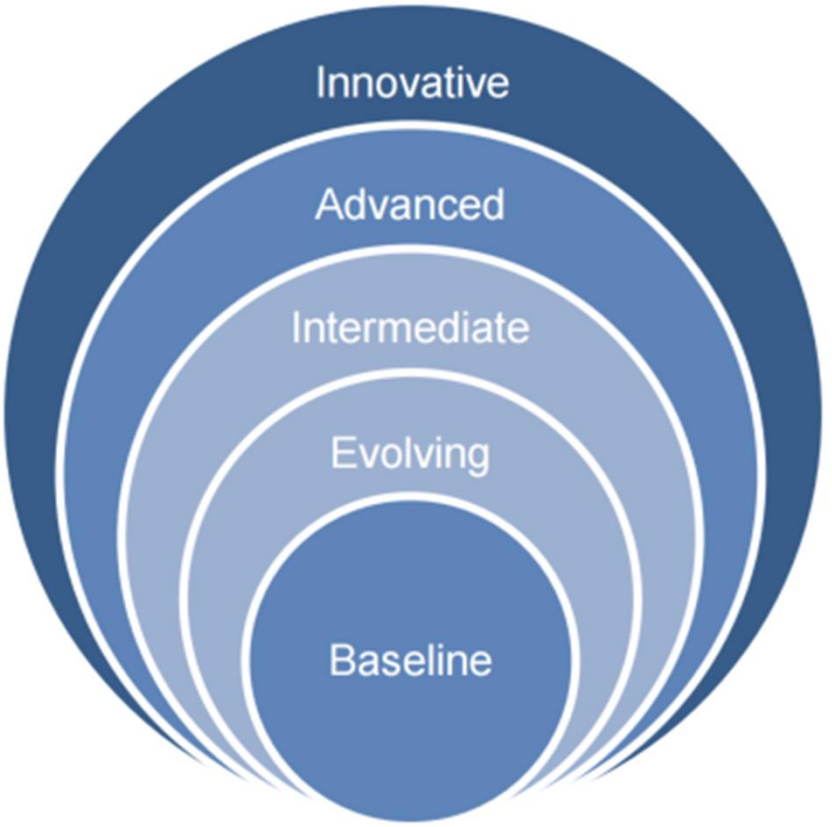


©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

How does Cybersecurity Maturity work?

Measured by 5 Cybersecurity Maturity Levels

1. Baseline
2. Evolving
3. Intermediate
4. Advanced
5. Innovative



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Declarative Statements

- Are the risk mitigating controls in your program
- 494 overall declarative statements

	Domain 1	Domain 2	Domain 3	Domain 4	Domain 5	Total
Baseline	31	8	51	16	17	**123**
Evolving	34	7	39	13	20	**113**
Intermediate	33	11	39	9	21	**113**
Advanced	28	11	25	7	15	**86**
Innovative	15	8	20	6	10	**59**
	141	**45**	**174**	**51**	**83**	**494**

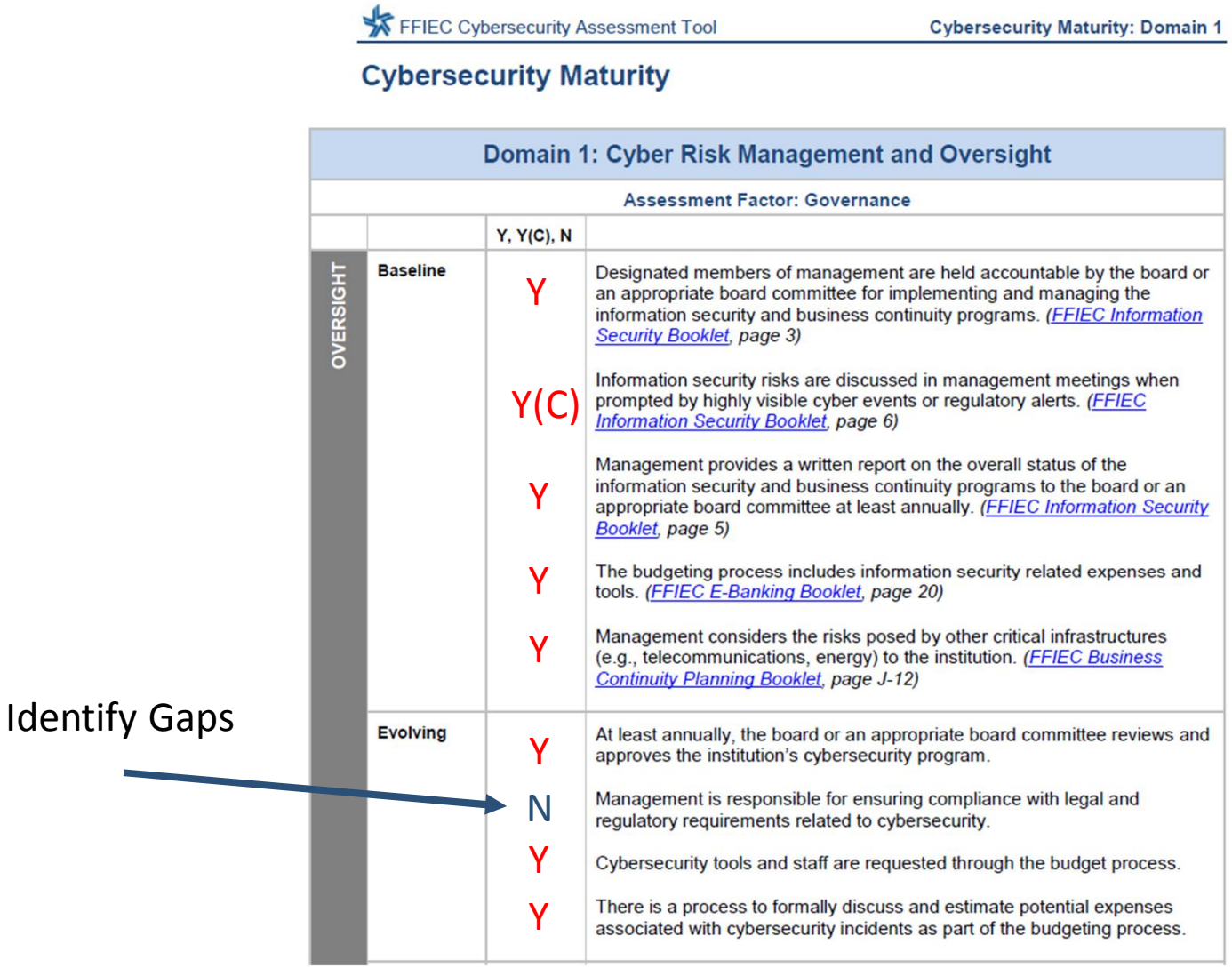
©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Compensating Controls!

- ***All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.*** Attained and sustained requires affirmative answers to either "Yes" or "Yes with Compensating Controls" for each of the declarative questions within a maturity level.
- **Compensating control** - A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in **lieu of a recommended security control** in the low, moderate, or high baselines that **provides equivalent or comparable protection** for an information system.

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Answer Declarative Statements



FFIEC Cybersecurity Assessment Tool — Cybersecurity Maturity: Domain 1

Cybersecurity Maturity

Domain 1: Cyber Risk Management and Oversight			
Assessment Factor: Governance			
		Y, Y(C), N	
OVERSIGHT	Baseline	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)*
		Y(C)	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 6)*
		Y	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)*
		Y	The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)*
		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)*
	Evolving	Y	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.
		N	Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.
		Y	Cybersecurity tools and staff are requested through the budget process.
		Y	There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.

Identify Gaps

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

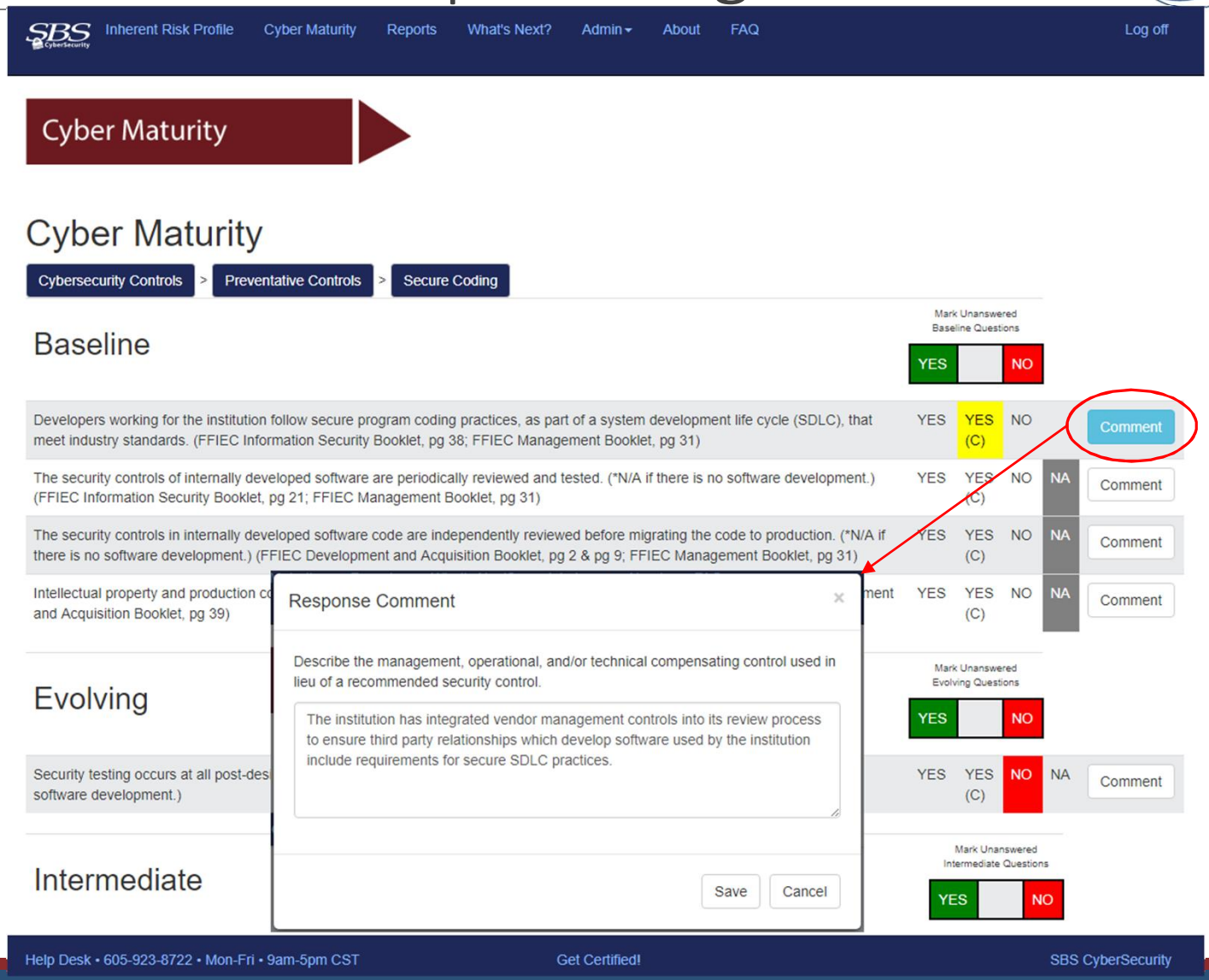
Compensating Controls (PCI)

According to the PCI Council, compensatory controls must:

- 1) Meet the intent and rigor of the original stated requirement;
- 2) Provide a similar level of defense as the original stated requirement;
- 3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- 4) Be commensurate with the additional risk imposed by not adhering to the original stated requirement.
- http://whatis.techtarget.com/definition/compensating-control

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Document Compensating Controls



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Appendix B: Compensating Controls:

Cybersecurity Controls

Preventative Controls

Access and Data Management

Access controls include password complexity and limits to password attempts and reuse. (FFIEC Information Security Booklet, pg 15)

Access controls do not address password reuse and attempt lockouts but workstation systems are protected by complex passwords and multifactor smart card authentication.

Preventative Controls

Secure Coding

Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. (FFIEC Information Security Booklet, pg 38; FFIEC Management Booklet, pg 31)

The institution has integrated vendor management controls into its review process to ensure third party relationships which develop software used by the institution include requirements for secure SDLC practices.

Detective Controls

Event Detection

Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. (FFIEC Information Security Booklet, pg 2)

The institution monitors for unauthorized hardware and software using an automated product from Manage Engine. Connections are monitored by our Intrusion Prevention System and user access is periodically reviewed manually.

Corrective Controls

Patch Management

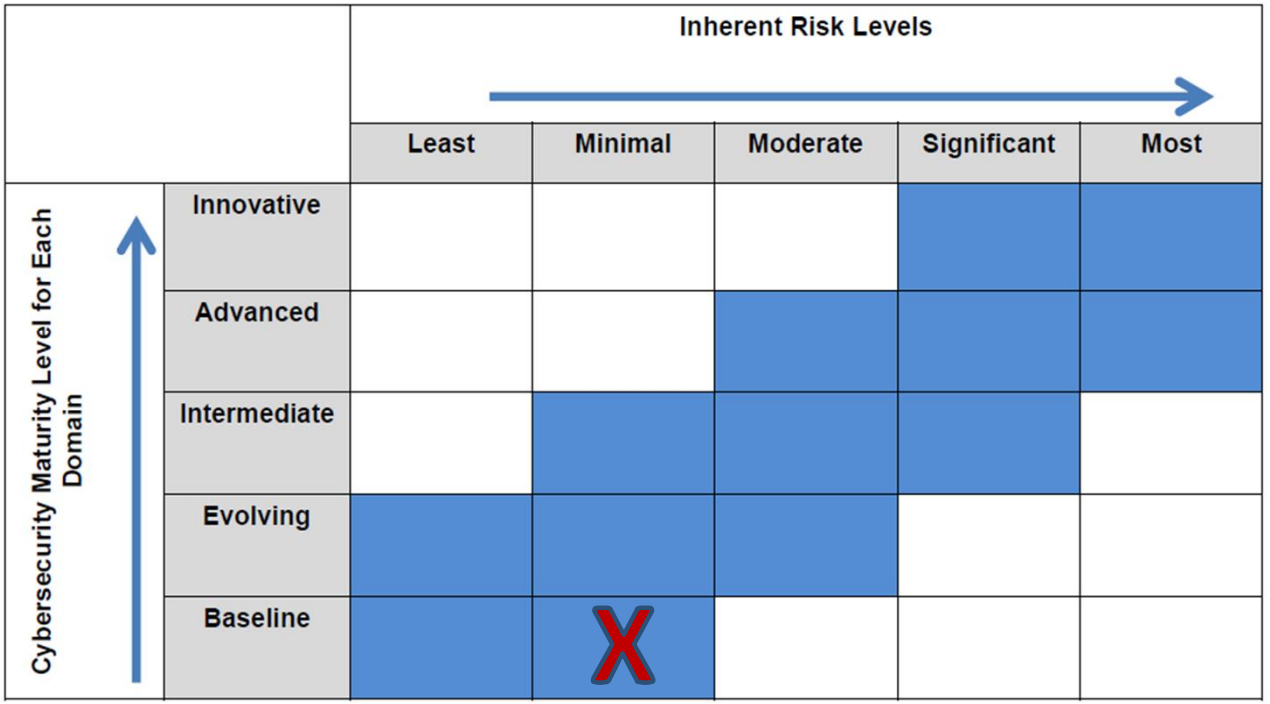
Patches are tested before being applied to systems and/or software. (FFIEC Operations Booklet, pg 22)

A dedicated testing environment cannot be established given limited resources. However, patched are deployed in a stage process, to minimum operational risk and use existing systems and software to test prior to rolling out updates on all systems.

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Determining IR vs. CS Maturity

Table 3: Risk/Maturity Relationship

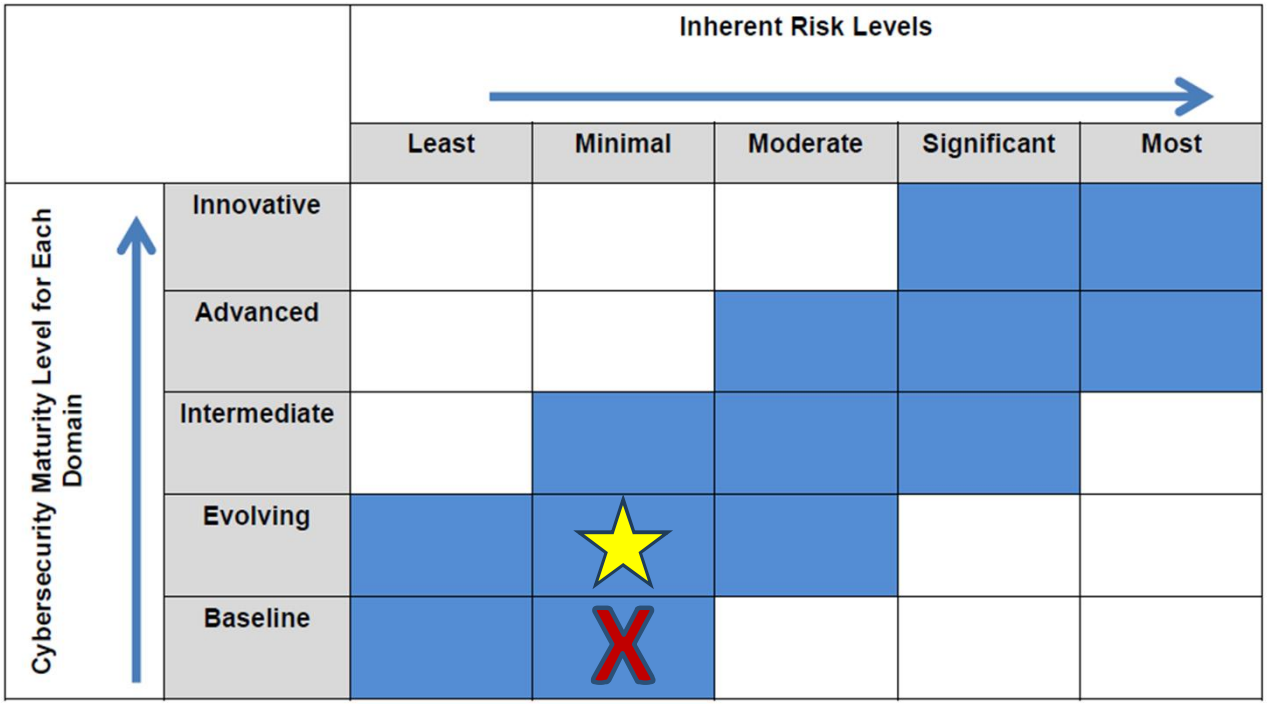


Domain 1: Cyber Risk Management and Oversight
Domain 2: Threat Intelligence and Collaboration
Domain 3: Cybersecurity Controls
Domain 4: External Dependency Management
Domain 5: Cyber Incident Management and Resilience

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Increasing Maturity

Table 3: Risk/Maturity Relationship



Domain 1: Cyber Risk Management and Oversight
Domain 2: Threat Intelligence and Collaboration
Domain 3: Cybersecurity Controls
Domain 4: External Dependency Management
Domain 5: Cyber Incident Management and Resilience

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Lessons Learned

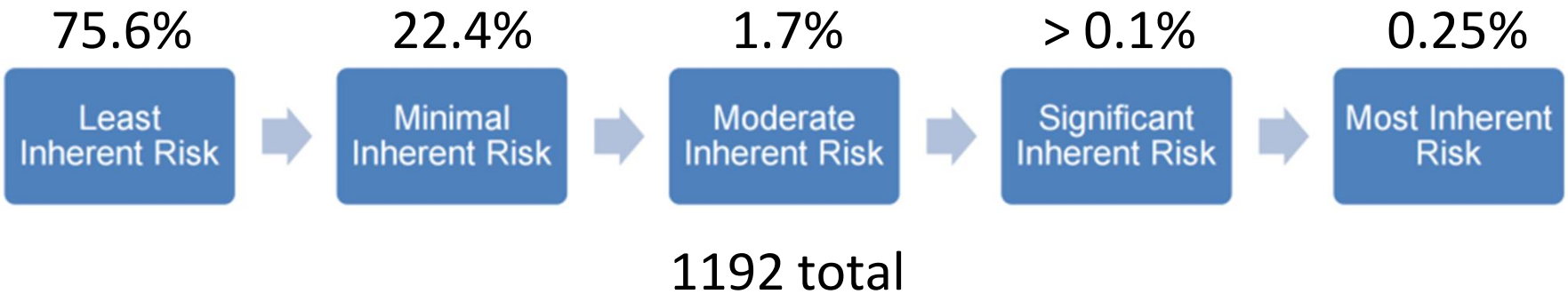
FDIC'S INFORMATION TECHNOLOGY RISK EXAMINATION PROCEDURES – WHAT YOU NEED TO KNOW

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Cybersecurity Inherent Risk

Å Five Inherent Risk Areas (39 Questions)

1. Technologies and Connection Types
2. Delivery Channels
3. Online/Mobile Products and Technology Services
4. Organizational Characteristics
5. External Threats



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Orgs Meeting Maturity Levels

	Domain 1: Cyber Risk Management & Oversight	Domain 2: Threat Intelligence & Collaboration	Domain 3: Cybersecurity Controls	Domain 4: External Dependency Management	Domain 5: Cyber Incident Management and Resilience
Below Baseline	43.9%	36.3%	54.9%	46.9%	43.9%
Baseline	56.1% (45.2%)	63.8% (46.6%)	45.1% (41.3%)	53.2% (43.1%)	56.1% (45.6%)
Evolving	10,9% (9.7%)	17.2% (14.9%)	3.8% (2.5%)	10.1% (7.0%)	10.5% (8.1%)
Intermediate	0.7%	1.2%	0.8%	1.1%	1.1%
Advanced	0.2%	0.7%	0.3%	1.6%	0.8%
Innovative	0.3%	0.4%	0.2%	0.4%	0.5%

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Orgs SETTING Maturity Levels

	Domain 1: Cyber Risk Management & Oversight	Domain 2: Threat Intelligence & Collaboration	Domain 3: Cybersecurity Controls	Domain 4: External Dependency Management	Domain 5: Cyber Incident Management and Resilience
Baseline	79.8%	80.6%	80.2%	80.8%	80.4%
Evolving	16.4%	15.8%	16.2%	15.4%	15.9%
Intermediate	2.4%	2.2%	2.4%	2.4%	2.2%
Advanced	0.5%	0.4%	0.2%	0.3%	0.4%
Innovative	0.9%	1.0%	1.0%	1.0%	1.1%
Actually MEETING Goals	45.6%	55.4%	34.3%	44.7%	46.8%
NOT MEETING Goals	54.4%	44.6%	65.7%	55.2%	53.2%

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Domain 1 Baseline Controls Not Met (31 Total)

- Governance > Strategies and Policies
  1. **The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. (6% No)**
- Governance > IT Asset Management
  2. **A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. (6.25% No)**
  3. **Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. (6.25% No)**
- Resources > Staffing
  4. **Processes are in place to identify additional expertise needed to improve information security defenses. (5.43 % No)**
- Training and Culture > Training
  5. **Customer awareness materials are readily available (9.66% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 3 Domain 2 Baseline Controls Not Met (8 Total)

Å Threat Intelligence and Information

1. **The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT). (4.28% No)**
2. **Threat information is used to enhance internal risk management and controls. (4.38% No)**

Å Monitoring and Analyzing

3. **Audit log records and other security event logs are reviewed and retained in a secure manner. (4.25% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 12 Domain 3 Baseline Controls Not Met (51 Total)

- Preventative Controls > Access and Data Management
  1. **All passwords are encrypted in storage and in transit. (6.82% No)**
  2. **Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (5.86% No)**
  3. **Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. (6.33% No)**
- Preventative Controls > Device/End-Point Security
  4. **Controls are in place to restrict the use of removable media to authorized personnel. (9.15% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 12 Domain 3 Baseline Controls Not Met (51 Total)

- Preventative Controls > Secure Coding
  5. **Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. (8.14% No)**
- Detective Controls > Threat and Vulnerability Detection
  6. **Firewall rules are audited or verified at least quarterly. (11.83% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 12 Domain 3 Baseline Controls Not Met (51 Total)

- Detective Controls > Anomalous Activity Detection
  7. **Access to critical systems by third parties is monitored for unauthorized or unusual activity. (7.3% No)**
  8. **Elevated privileges are monitored. (7.89% No)**
  9. **The institution is able to detect anomalous activities through monitoring across the environment. (7.52%)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 12 Domain 3 Baseline Controls Not Met (51 Total)

- Detective Controls > Event Detection
  10. **A normal network activity baseline is established. (11.26% No)**
  11. **Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. (9.27% No)**
- Corrective Controls > Patch Management
  12. **Patches are tested before being applied to systems and/or software. (7.89% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Domain 4 Baseline Controls Not Met (16 Total)

- Connections > Connections
  1. **Data flow diagrams are in place and document information flow to external parties. (15.16% No)**
- Relationship Management > Contracts
  2. **Contracts establish responsibilities for responding to security incidents. (8.37% No)**
  3. **Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements. (7.87% No)**
  4. **Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. (7.76% No)**
- Relationship Management > Ongoing Monitoring
  5. **Ongoing monitoring practices include reviewing critical third-parties' resilience plans. (7.46% No)**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Domain 5 Baseline Controls Not Met (17 Total)

- Incident Resilience Planning and Strategy > Planning
  1. **The institution has documented how it will react and respond to cyber incidents. (6.16% No)**
- Incident Resilience Planning and Strategy > Testing
  2. **Business continuity testing involves collaboration with critical third parties. (6.96% No)**
  3. **Scenarios are used to improve incident detection and response. (6.48% No)**
- Detection, Response, and Mitigation > Detection
  4. **System performance reports contain information that can be used as a risk indicator to detect information security incidents. (7.57% No)**
  5. **Tools and processes are in place to detect, alert, and trigger the incident response program. (6.88% No)**

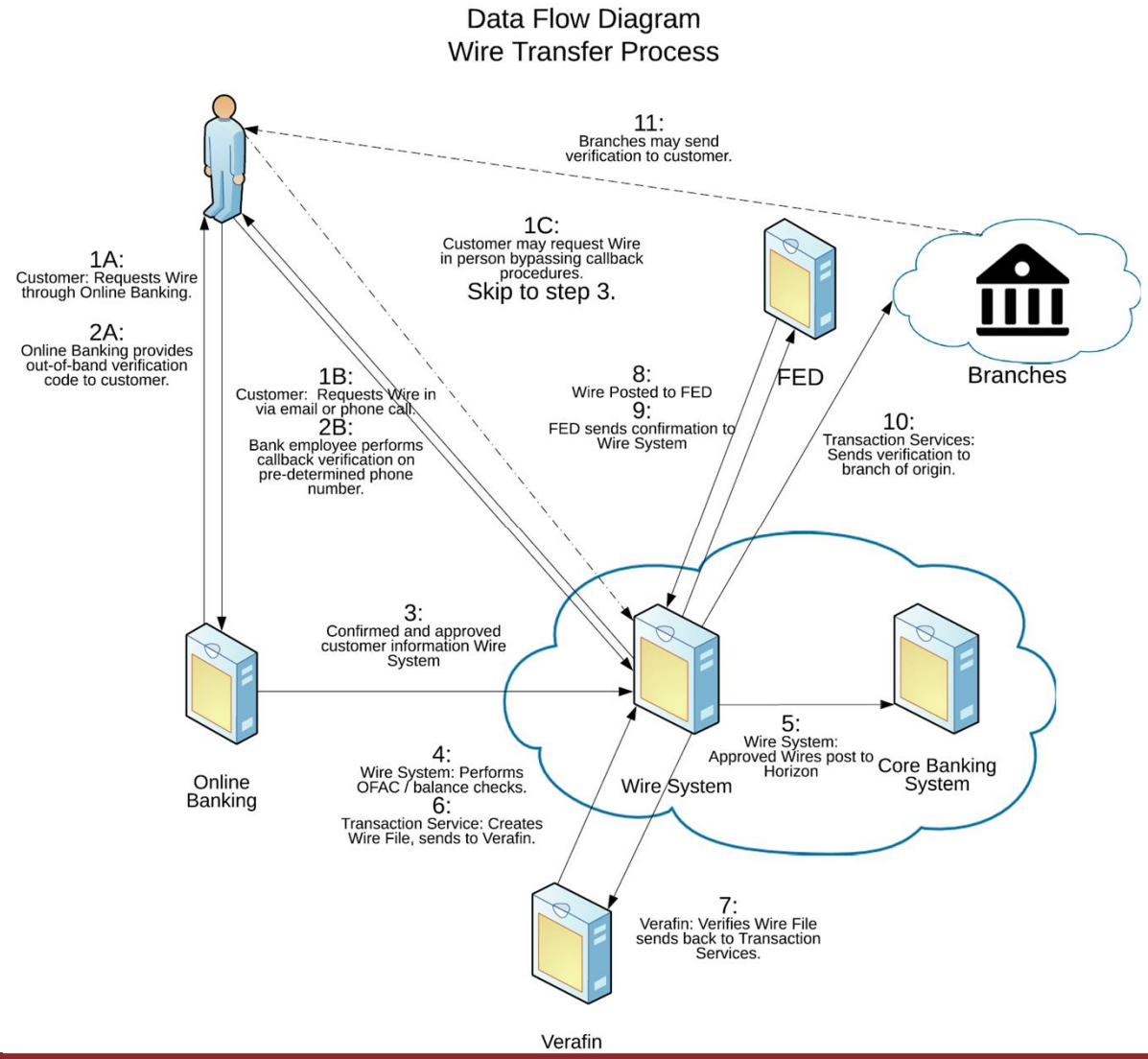
©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

5 Biggest Baseline "No" Offenders

1. **Data flow diagrams** are in place and document information flow to external parties. **(15.16% No)** (Domain 4)
2. **Firewall rules are audited or verified at least quarterly**. **(11.83% No)** (Domain 3)
3. The **institution is able to detect anomalous activities** through monitoring across the environment. **(11.26% No)** (Domain 3)
4. **Customer awareness materials** are readily available **(9.66% No)** (Domain 1)
5. Processes are in place to **monitor for the presence of unauthorized users, devices, connections, and software**. **(9.27% No)** (Domain 3)

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

#1 – Data Flow Diagram



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

#2 - Quarterly Firewall Review

- Look for changes in current firewall rules vs. previous firewall rules
- Evaluate firewall **change management** procedures, logging of rule changes, and the adequacy of the change management process
- Look for any rules that seem out of place or odd
- Resolving external IPs that are specifically called out or allowed in rules
- Look for hard-coded passwords in rules
- Evaluating open ports and the business need of said open ports

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

#3 - Detect Anomalous Activity

- How would you know if someone was in your network?
- Do you have Key Risk Indicators in place?
  - Total Network Logs per Second
  - Patch Management % / Known Vulnerabilities
  - Denied FTP Requests
  - Denied Telnet Requests
  - Failed Remote Logins
  - VPN Connections / Failed VPN Connections
  - Blacklisted IP's Blocked
  - New Admin Credentials created
  - Threshold for successive account lockouts
  - VLAN ACL violations
  - Changes to Group Policy
  - Increase in network bandwidth
  - Increase in outbound email traffic
  - DNS Request anomalies

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

#4 – Customer Security Awareness

- SANS Securing the Human: https://www.sans.org/security-awareness-training/
- SBS CyberSecurity Free Downloads: https://sbscyber.com/education/free-downloads
- Hang up Security Awareness Posters around your buildings (Google some free posters)
- Send out regular newsletters and have conversation with customers over social media

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

#5 – Detect New Stuff on your Network

- Start with having (and keeping) and up-to-date Asset Inventory
- Look into automating said asset inventory
- Get alerts when new things are found on the network or on your devices
- Detection is just as important as protection

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Y(CC) Baseline Controls

Å Cybersecurity Controls > Preventative Controls > Access and Data Management

1. **Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data.**
   (22 instances - 2.11% YCC)
   - **Most Y(CC) descriptions talk about mobile devices "not storing confidential information" but can *ONLY* access email or connect to the network via VPN**
   - **What is a TRUE Compensating Control?**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Y(CC) Baseline Controls

Å Cybersecurity Controls > Preventative Controls > Access and Data Management

2. **Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.**
   (21 instances – 2.02% YCC; 91.3% Yes; 6.3% No)
   - **Most Y(CC) descriptions discuss vendors using encryption but not MFA or "having to request access from the bank first"**
   - **What is a TRUE Compensating Control?**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Y(CC) Baseline Controls

Å Cybersecurity Controls > Preventative Controls > Secure Coding

3. **Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.**
   (49 instances – 4.75% YCC; 79% Yes; 8.1% No)
   - **Majority of Y(CC) descriptions discuss not having development capabilities internally; some reference Core Banking vendor**
   - **What is a TRUE Compensating Control?**
   - **This would certainly be a candidate for an N/A answer, depending on the interpretation of your regulator**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Y(CC) Baseline Controls

Å Cybersecurity Controls > Detective Controls > Threat and Vulnerability Detection

4. **Firewall rules are audited or verified at least quarterly.**
   (30 instances – 2.91% YCC; 85.3% Yes; 11.8% No)
   - **Most Y(CC) descriptions reference annual reviews, rather than quarterly; others reference logging of changes (but not verified) or the vendor managing the firewall**
   - **What is a TRUE Compensating Control?**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Top 5 Y(CC) Baseline Controls

Å Cybersecurity Controls > Corrective Controls > Patch Management

5. **Patches are tested before being applied to systems and/or software.**
   (31 instances – 3.02% YCC; 89.1% Yes; 7.9% No)
   - **Y(CC) descriptions include accepting the risk and the ability to roll-back; critical patches being applied "automatically", vendor testing, or scaled roll-out to "test" systems before rolling out to entire production network**
   - **What is a TRUE Compensating Control?**

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

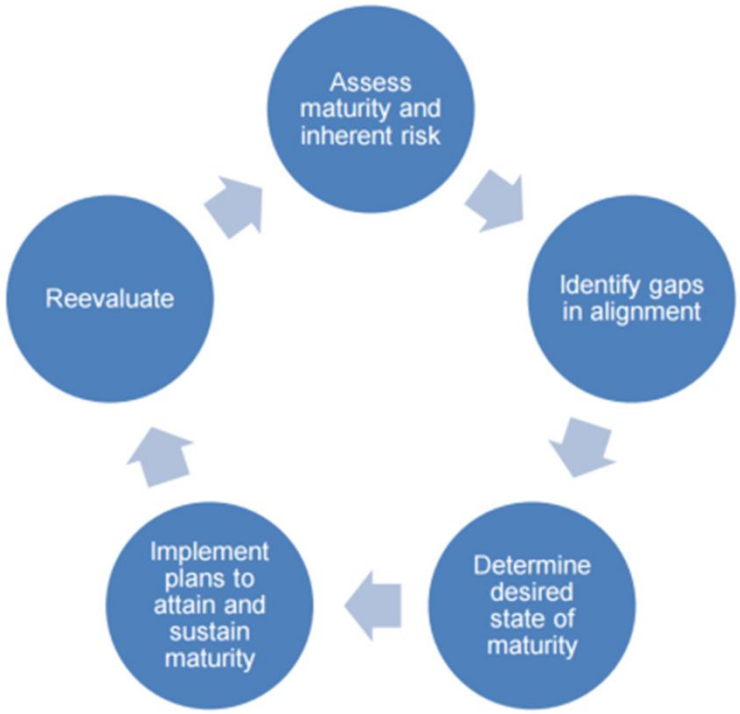
Next Steps

WHAT ARE THE NEXT STEPS TO FOLLOW AFTER YOU COMPLETE THE FFIEC CYBERSECURITY ASSESSMENT TOOL?

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Next steps?

1. ~~Determine Inherent Risk~~
2. ~~Determine Domain Maturity~~
3. ~~Identify Goals~~
4. Identify Gaps
5. Implement additional controls
6. Increase maturity
7. Repeat



©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Identify Gaps

Domain	Factor	Component	Statement	Level	Respons
Cybersecurity Controls	Preventative Controls	Device/End-Point Securit	Controls are in place to restrict the use of removable media to authorized pe	Baseline	No
Cybersecurity Controls	Preventative Controls	Secure Coding	Developers working for the institution follow secure program coding practice:	Baseline	No
Cybersecurity Controls	Preventative Controls	Secure Coding	The security controls of internally developed software are periodically review	Baseline	No
Cybersecurity Controls	Preventative Controls	Secure Coding	The security controls in internally developed software code are independentl	Baseline	No
Cybersecurity Controls	Preventative Controls	Secure Coding	Intellectual property and production code are held in escrow. (*N/A if there is	Baseline	No
Cybersecurity Controls	Detective Controls	Threat and Vulnerability I	Independent testing (including penetration testing and vulnerability scanning	Baseline	No
Cybersecurity Controls	Detective Controls	Threat and Vulnerability I	Antivirus and anti-malware tools are used to detect attacks. (FFIEC Informa	Baseline	No
Cybersecurity Controls	Detective Controls	Threat and Vulnerability I	Firewall rules are audited or verified at least quarterly. (FFIEC Information Se	Baseline	No
Cybersecurity Controls	Detective Controls	Threat and Vulnerability I	E-mail protection mechanisms are used to filter for common cyber threats (e	Baseline	No
Cybersecurity Controls	Detective Controls	Anomalous Activity Dete	The institution is able to detect anomalous activities through monitoring acr	Baseline	No
Cybersecurity Controls	Detective Controls	Anomalous Activity Dete	Customer transactions generating anomalous activity alerts are monitored a	Baseline	No
Cybersecurity Controls	Detective Controls	Anomalous Activity Dete	Logs of physical and/or logical access are reviewed following events. (FFIEC	Baseline	No
Cybersecurity Controls	Detective Controls	Anomalous Activity Dete	Access to critical systems by third parties is monitored for unauthorized or	Baseline	No
Cybersecurity Controls	Detective Controls	Anomalous Activity Dete	Elevated privileges are monitored. (FFIEC Information Security Booklet, pag	Baseline	No
Cybersecurity Controls	Detective Controls	Event Detection	A normal network activity baseline is established. (FFIEC Information Secur	Baseline	No
Cybersecurity Controls	Detective Controls	Event Detection	Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert mar	Baseline	No
Cybersecurity Controls	Detective Controls	Event Detection	Processes are in place to monitor for the presence of unauthorized users, d	Baseline	No
Cybersecurity Controls	Detective Controls	Event Detection	Responsibilities for monitoring and reporting suspicious systems activity ha	Baseline	No
Cybersecurity Controls	Detective Controls	Event Detection	The physical environment is monitored to detect potential unauthorized acc	Baseline	No
Cybersecurity Controls	Corrective Controls	Patch Management	A patch management program is implemented and ensures that software ar	Baseline	No
Cybersecurity Controls	Corrective Controls	Patch Management	Patches are tested before being applied to systems and/or software. (FFIEC	Baseline	No
Cybersecurity Controls	Corrective Controls	Patch Management	Patch management reports are reviewed and reflect missing security patche	Baseline	No
Cybersecurity Controls	Corrective Controls	Remediation	Issues identified in assessments are prioritized and resolved based on critic	Baseline	No
External Dependency Management	Connections	Connections	The critical business processes that are dependent on external connectivity	Baseline	No
External Dependency Management	Connections	Connections	The institution ensures that third-party connections are authorized. (FFIEC I	Baseline	No
External Dependency Management	Connections	Connections	A network diagram is in place and identifies all external connections. (FFIE	Baseline	No
External Dependency Management	Connections	Connections	Data flow diagrams are in place and document information flow to external p	Baseline	No
External Dependency Management	Relationship Manageme	Due Diligence	Risk-based due diligence is performed on prospective third parties before co	Baseline	No
External Dependency Management	Relationship Manageme	Due Diligence	A list of third-party service providers is maintained. (FFIEC Outsourcing Boo	Baseline	No
External Dependency Management	Relationship Manageme	Due Diligence	A risk assessment is conducted to identify criticality of service providers. (F	Baseline	No

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

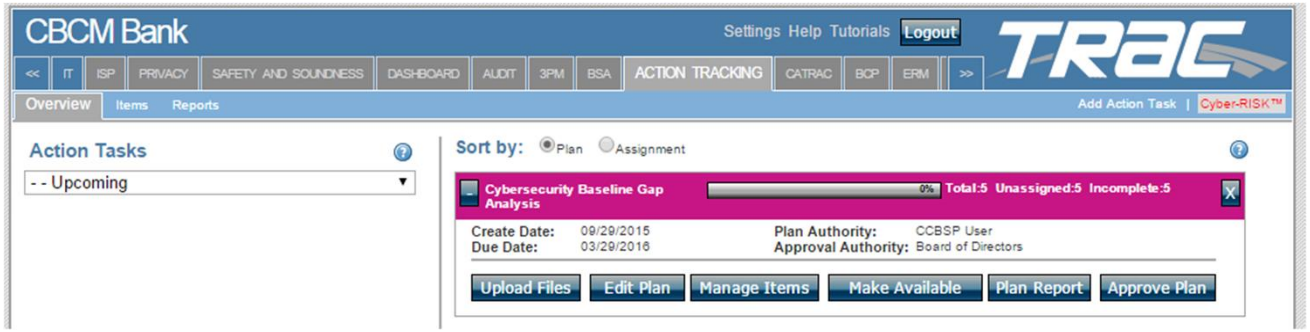
Maturity Next Steps

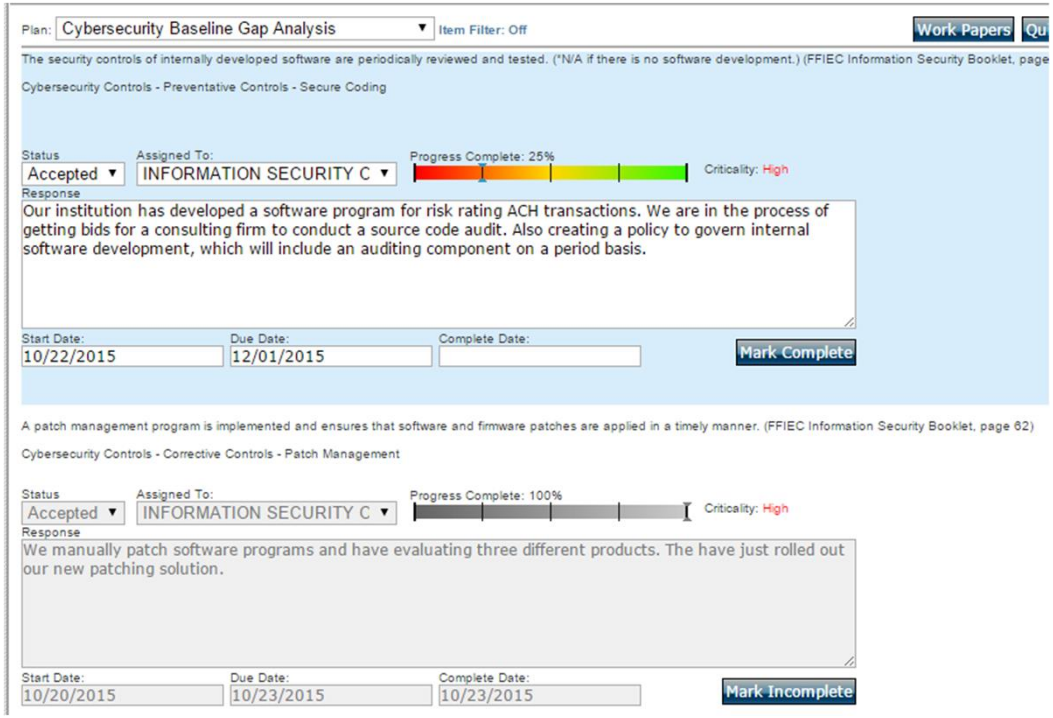
- You don't have to set a goal for EVERY one of the 5 Domains. If you have 2 or 3 Domains to work towards maturing, that's plenty to do for the next 6-12 months. Meeting some of your goals for now is OK.
- Include timeframes, budget, priorities, etc.
- Report Upstream

Cyber Maturity Level	Statements Needed
Baseline	
Cyber Risk Management and Oversight	***6***
Threat Intelligence and Collaboration	***0***
Cybersecurity Controls	***4***
External Dependency Management	***0***
Cyber Incident Management and Resilience	***1***

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Build Action Plan





©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Biggest Takeaways

- Only 55% of nearly 1200 organizations that have completed the CAT (in Cyber-RISK) are meeting baseline standards
- Only about 1% of all responses are utilizing the Yes with Compensating Controls feature
  - And those that ARE using Y(CC) are not using it correctly

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Biggest Takeaways

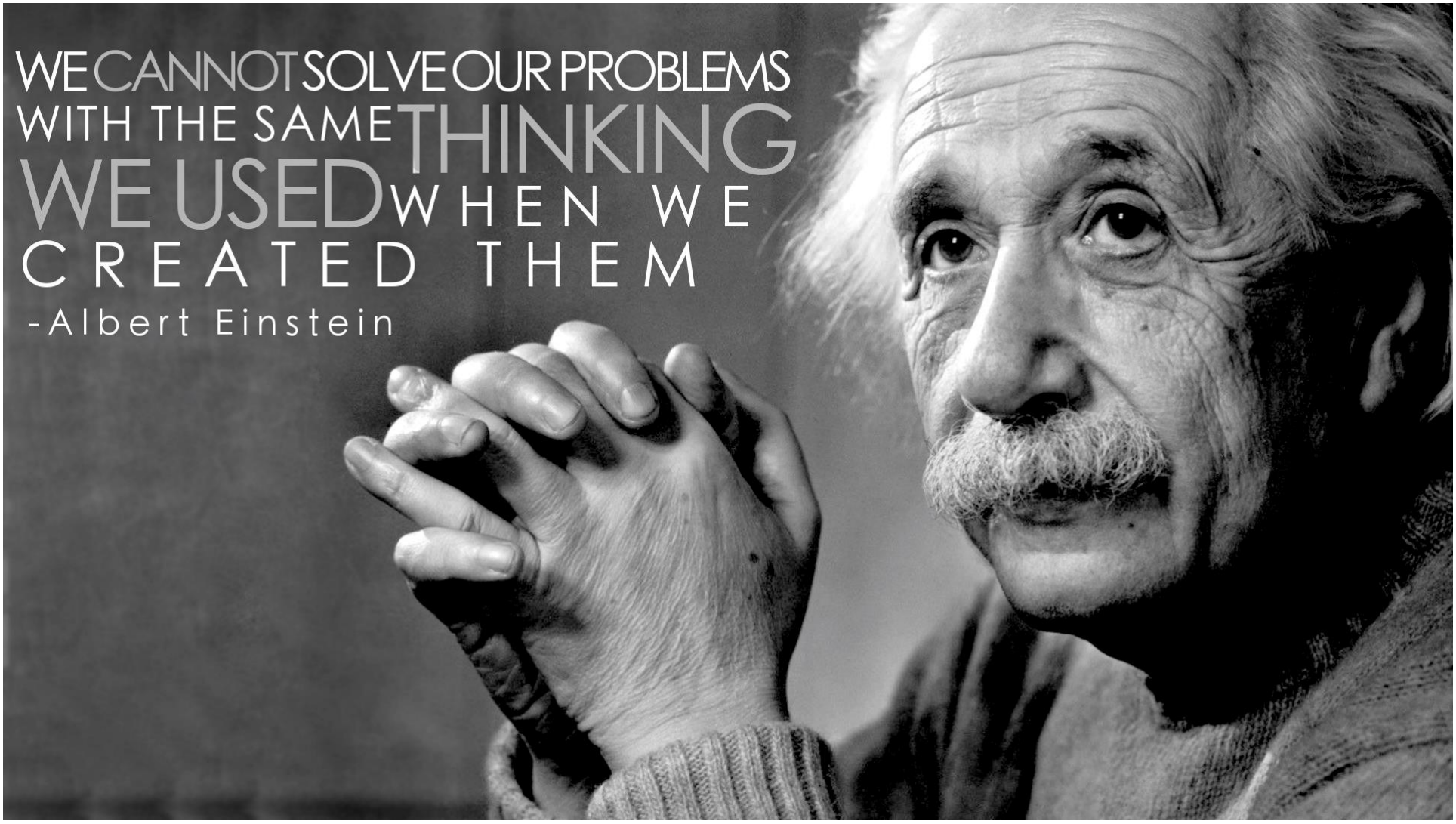
- It's ok to not be meeting Baseline, AS LONG AS YOU HAVE A PLAN.

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com

Biggest Takeaways

- A LOT of effort spent on completing the CAT – make sure it's **VALUABLE**
  - Over 500,000 answers to CAT maturity questions
  - If you assume 10 minutes per question, that's over **5 MILLION minutes** put into the CAT by users of Cyber-RISK
    - Over 83,000 hours – or almost 3500 days – or 9.5 years…
  - Take that 2X if you've completed the CAT twice
- Use the CAT to PLAN the MATURITY of your Information Security Program

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com



©2018 SBS CyberSecurity, LLC www.sbscyber.com

That's all she wrote…

- Any questions, comments, or concerns?
- Also, for a much deeper dive on Cybersecurity *specifically* for financial institutions, check out our eleven (11) **Cybersecurity Certification Programs**!
  - Including the **Certified Banking Cybersecurity Manager**
  - **https://sbscyber.com/education/certifications**
- Contact info:
  - Jon Waldman
  - Partner, EVP IS Consulting
  - jon.waldman@sbscyber.com
  - 605-380-8897

©2018 SBS CyberSecurity, LLC
https://www.sbscyber.com