



ABC Sample Company

NIST Sample Presentation

NIST Framework

This risk assessment follows the Center for Internet Security (CIS) 20 framework of cyber security. These are 20 controls that, when followed, provide multiple layers of depth for defense and policy. This framework is mainly aimed at the technical aspects of Information and Cyber Security with some lighter focus on policy.

ABC Sample Company

High-Level Observations

Ascend Technologies was engaged to conduct a cybersecurity risk assessment for ABC. Ascend spent several hours over a weeklong period with ABC and outsource vendor XYZ, discussing the current state of the IT Security program and capabilities at ABC. The driving purposes for the risk assessment are 3rd Party vendor assessment requests and client confidence in ABC.

Below are high level observations from those discussions:

- *Exposed critical business application(s)*
- *Limited commercial grade protective technology*
- *Limited commercial grade detective technology*
- *No dedicated security staff (existing IT staff spends ~10% of time on security)*
- *No real time security monitoring in place for security systems, applications or threat detection*
- *No security awareness and training program*
- *No incident response program*
- *No vulnerability management program*
- *Unsecured access to user workstations/laptops*
- *No multifactor authentication to critical business applications*
- *Users have local administrator access to workstations/laptops*
- *No formal security program*
- *No documented security strategy*
- *No security risk management program*
- *No formal workstation/laptop patching program*
- *No system or data redundancy to guard against data loss or system failures*

ABC Sample Company

Prioritized Security Project to Address Urgent Concerns

Projects:

Protection of Critical Application (Client Management System) – protect critical client systems and data

- Identify critical applications and data
- Isolate application and database servers
- System hardening and application database encryption
- Enhance security protection and monitoring of core applications
- Next Generation Firewall protection
- Application penetration testing

Improve Endpoint Protections – protect devices that are accessing critical client information

- Password protected access to workstations/laptops
- Replace freeware with commercial anti-virus and malware protections
- Patch endpoints on a monthly basis

Security Awareness and Training – educate users on how to identify and avoid potentially harmful actions

- Identify cloud vendors for security awareness training
- Evaluate and select vendor
- Create training calendar; Rollout training to end users
- Email Security Protection

Security Incident Response – institute a plan for how to react to a security incident

- Develop incident response plan
- Execute tabletop exercise to test plan

Multifactor Authentication – enhance access controls to critical systems and data

- Identify scope for MFA application
- Identify, evaluate and implement solutions

Perimeter and Firewall Architecture Review – improve security protection capabilities

- Evaluate hardware configuration and firewall rules

Email and Exchange Online Security Review – protect sensitive email data

- Evaluate Email Gateway configuration and rule base
- ABC is in the process of moving from on premise Exchange email to Exchange online
- Evaluate the configuration and migration plan for securely moving ABC email

ABC Sample Company

Prioritized Security Programs to Address Gaps

Programs:

Engage Managed Provider (24x7 SOC Monitoring and Incident Response)

- Next-Generation Firewalls
- Malware Protection
- Email Security Management
- Network Monitoring System
- Endpoint Encryption
- Endpoint Detection and Response (EDR)

Vulnerability Management Program

- Identify vulnerability scanning tools (web and network)
- Evaluate tools, select solution
- Design and implement recurring scanning of critical systems and applications
- Implement remediation program and patch management solution

Cybersecurity Governance Program




- Institute a risk management approach to ABC's Security program
- Develop security strategy for reaching appropriate security posture
- Develop metrics for measuring security posture and success criteria
- Develop and implement security policies and procedures
- Execute on security governance program




Enhance End point Security

- Remove local administrator access from workstations/laptops
- Join workstations/laptops to Active Directory domain
- Deploy endpoint management solution (MDM)

Penetration Testing Program

- Identify penetration testing vendors (systems and application)
- Selection and engage vendor for initial evaluation
- Implement recurring penetration testing of select systems and applications

IMPACT LEGEND  LOW  MODERATE  HIGH

COMPLEXITY LEGEND  LOW  MODERATE  HIGH

Prioritized Recommendations	One-Time Cost	Ongoing Cost (Annual)	Duration (Months)	Impact	Complexity		
Projects							
Protection Critical Application (includes next generation firewall and threat protection)			3-6				
Improve Endpoint Protections			2-3				
Security Awareness and Training (includes improved email protection)			3-6				
Security Incident Response			3-4				
Multifactor Authentication			4-6				
Security Architecture Review			.5-1				
Exchange Online Security Review			2-3				
Programs							
Managed Security Services					2-3		
Vulnerability Management Program					2-3		
Cybersecurity Governance Program			3-6				
Enhance Endpoint Security			3-6				
Penetration Testing Program			1-2				







ABC Sample Company

Cybersecurity Risk Assessment Results

Threats and Vulnerabilities

The most substantial threats to the organization is the exposure of sensitive information, such as company data, client data, or employee data. These top threats should be the focus of security maturity improvement efforts

	Impact	Resilience
Ransomware	 <p>Low High</p>	In the event of a ransomware attack, the organization would be most impacted if its primary business application and/or the supporting subsystems were controlled by an attacker. The organization should have a documented disaster recovery plan that integrates with a documented business continuity plan. These should be routinely tested to ensure the most critical applications and supporting systems can be recovered within the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
Insider Threat	 <p>Low High</p>	The company stores a significant amount of sensitive client data on their Client Management System (CMS). A comprehensive data protection program that enhances the protection and monitoring controls over sensitive information can significantly increase the ability to trace inappropriate and unauthorized use and access to sensitive data.
Targeted Phishing	 <p>Low High</p>	Many organizations have experienced an uptick in phishing attempts. Email filtering helps to protect the internal environment. Company-wide security awareness training and phishing campaigns are important in order to educate end users to reduce the risk.
Business Email Compromise	 <p>Low High</p>	Most companies rely on its email platform for communications. Sensitive financial and business information are contained within or relayed via this channel. Compromise of the email platform may also be used as reconnaissance to attack critical systems.

A Standardized Cybersecurity Framework

Ascend Technologies' security risk analysis focuses on security controls across six key domains based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)



IDENTIFY

What are you defending and who are you defending against?



PROTECT

How do you block an attack?



DETECT

How are you monitoring and finding security concerns?



RESPOND

What decisions need to be made and how do you make them?



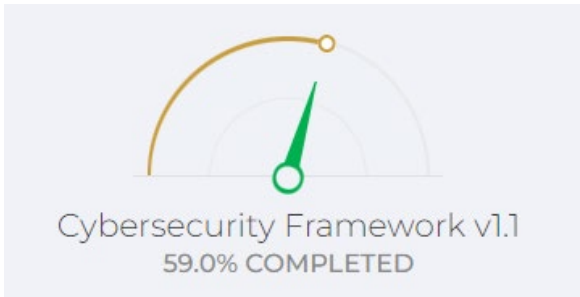
RECOVER

What needs to be recovered and how do you do it?

ABC Sample Company Risk Profile



Results



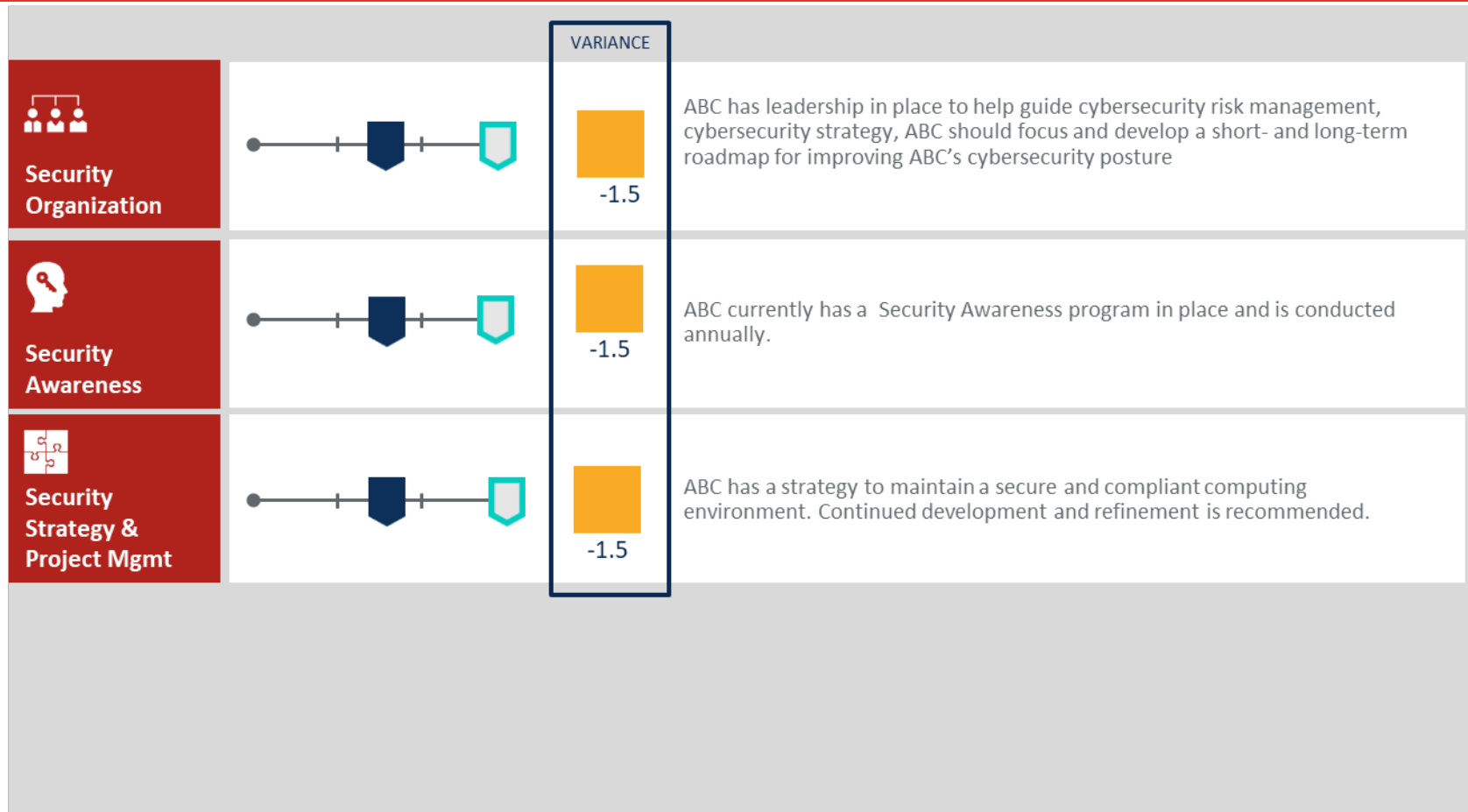
Security Maturity Ratings (1 of 5)

Security Organization and Strategy

MATURITY RATING LEGEND

CURRENT STATE

DESIRED FUTURE STATE



MATURITY RATING VARIANCE LEGEND

0 MODERATE

<2 MODERATE

>= 2 LOW













EQUIVALENT MATURITY LEVEL HIGH MODERATE LOW

13

Security Maturity Ratings (2 of 5)

Security Operations and Policies

LEGEND  CURRENT STATE  DESIRED FUTURE STATE



		VARIANCE	
 Documented Policies & Procedures		 -1	IT security policies need to be further documented. Procedures will need to be developed to ensure the consistent application of each policy. Policies and procedures are operationalized and communicated.
 Risk & Vulnerability Management		 -1	ABC does assess cybersecurity risk but does not have documented process or tolerances established. In order to identify areas of concern and to guide the cybersecurity strategy risk assessments are critical. Penetration testing and vulnerability scanning are key components of a good Risk & Vulnerability Management program. Continue communicating the overall Cybersecurity Risk Management program to ABC Management.
 Change Management		 -1	Changes made to critical IT systems and critical business applications should be fully documented and approved by committee or IT director. The change request should include the change justification, testing procedures and results, analysis of potential impacts and security implications, rollback plans and post-change validation testing.
 Asset Management		 -1	Knowing what assets you need to protect is key to cybersecurity. Asset management for ABC is currently an undocumented process with limited proof. ABC should define and implement processes for improving the completeness, accuracy and integrity of the inventory.













MATURITY RATING  0  <2  >=2

VARIANCE LEGEND

Security Maturity Ratings (3 of 5)

Security Operations and Policies

LEGEND  CURRENT STATE  DESIRED FUTURE STATE

		VARIANCE	
 IT Security Incident Response		 -1	Incident response management and response policies is drafted and approved. The IT Manager is the leader of the IR Event Management Team. Once the IR policies have been approved, training for the key members of the team and a tabletop exercise will be important to the success of an ABC Incident Response Plan.
 Configuration Management		 -1	The Internal IT team has processes and configurations for deploying IT assets, however these activities have been formally documented, but updating is inconsistent. Common configurations are applied to workstations and servers and do account for security hardening requirements. Continuous monitoring of configurations on critical systems and applications is also employed.
 Vendor Management		 -1	A vendor management policy and processes are documented to cover key vendor relationships. Vendors are required to sign non-disclosure agreements and contracts as well.
 Disaster Recovery/Biz Continuity Plan		 -1	A documented disaster recovery nor business continuity plan is currently in place at ABC. Development of testing and yearly assessment should continue.

MATURITY RATING
VARIANCE LEGEND



0





<2















>=2

Security Maturity Ratings (4 of 5)

Security Technology

LEGEND  CURRENT STATE  DESIRED FUTURE STATE

		VARIANCE	
 Network Security		 -1	ABC does monitor the performance and availability of their network infrastructure. Network security is a part of the infrastructure. This is being covered by the next generation firewalls and Cisco AMP for security. Network segmentation is used in the environment to enhance the network protections by preventing lateral movement if intruders do access one of the segments.
 Identity & Access Management		 -.5	Active Directory is leveraged to verify, identify and facilitate access management across the organization. Accounts and privileges are reviewed on a semi-annual basis. Access to laptops and desktops are controlled. MFA is utilized. The policy of least privileged access is implemented.
 Data Management		 -.8	Policies should be developed to formally establish data sensitivity levels and classifications. Sensitive data locations and a formal information asset inventory should be performed which is a prerequisite to a data loss prevention program. The implementation of network-level data loss prevention (DLP) technology will aid in the reduction of data protection risk.
 Patch Management		 -1	ABC has a documented process for deploying patches on workstations. IT department manages patching for servers and network devices. Remote deployment of patches are often relied upon to patch applications as patches are released. Third party application (e.g. Java, Adobe) patching is completed every 6 months after evaluation. Enhancing ABC's tool kit will help to reduce the risk vulnerabilities going unpatched.

MATURITY RATING
VARIANCE LEGEND

 0
EQUIVALENT MATURITY LEVEL HIGH













 <2
MODERATE

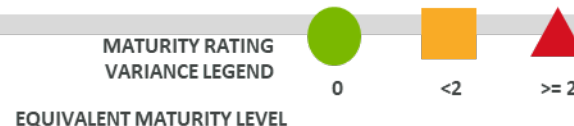
 >= 2
LOW

Security Maturity Ratings (5 of 5)

Security Technology

LEGEND  CURRENT STATE  DESIRED FUTURE STATE

		VARIANCE	
 Logging/ Monitoring		 -0.5	ABC does not have a full-time staffed Security Operations Center (SOC). A Security Information and Event Management (SIEM) solution and active workstation monitoring is implemented to provide real-time visibility and alerting. ABC would benefit from having a SOC that monitors their environment 24x7x365 to detect real-time events indicative of a breach.
 Physical Security		 -1	The ABC building manages badges for accessing offices and restricted areas. Key cards are required for data center access. A control list of physical keys are kept for off campus locations.
 Endpoint Security		 -1	Symantec Endpoint, Cisco AMP and careful firewall policies are in place and utilized for endpoint security. Logs are aggregated into a SIEM and detection rules are in place.
 Network Architecture		 -1	ABC's corporate and production environments are logically separated. The ABC network is segmented using virtual local area networks (VLANs) based on business purpose and system security profiles.





Questions?

teamascend.com