RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

#RSAC

SESSION ID: STR-W14

BUILDING AND SELLING YOUR SECURITY STRATEGY: A CASE STUDY

Rick Patterson

Head of Security Operations
Financial Services
@rpatterson123

Overview

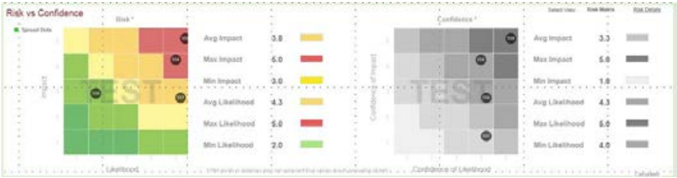
- Why is this important
- How (Case Study-ish)
  - Build a risk Framework
  - Get Business buy-in
  - Customize a Control Framework
  - Develop Tooling
- Benefits to your Organization
- Key takeaways
- Application

Why is this important

- It is the building block for a risk based security strategy
- Helps answers questions on why you need funding and for what
- Protects your budget
- Source of additional funding for critical risk remediation
- Helps answers threat questions within a framework
- Protects you and your team from being the fall guy (unless you deserve it)

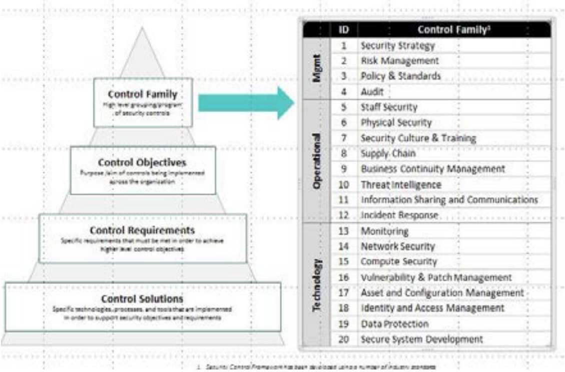
How to sell our security strategy

- Four critical components
  - Risk Framework
  - Business buy-in/support
  - Customized control framework
  - Tooling



Risk vs Confidence

	Risk		Confidence
Avg Impact	3.8	Avg Impact	3.3
Max Impact	5.0	Max Impact	5.0
Min Impact	3.0	Min Impact	1.0
Avg Likelihood	4.3	Avg Likelihood	4.3
Max Likelihood	5.0	Max Likelihood	5.0
Min Likelihood	2.0	Min Likelihood	4.0



Control Family
High level grouping/program of security controls

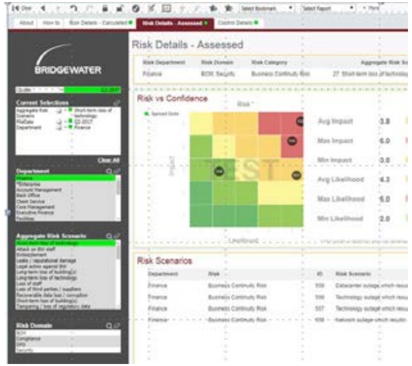
Control Objectives
Purpose /aim of controls being implemented across the organization

Control Requirements
Specific requirements that must be met in order to achieve higher level control objectives

Control Solutions
Specific technologies, processes, and tools that are implemented in order to support security objectives and requirements

	ID	Control Family[1]
Mgmt	1	Security Strategy
	2	Risk Management
	3	Policy & Standards
	4	Audit
Operational	5	Staff Security
	6	Physical Security
	7	Security Culture & Training
	8	Supply Chain
	9	Business Continuity Management
	10	Threat Intelligence
	11	Information Sharing and Communications
	12	Incident Response
Technology	13	Monitoring
	14	Network Security
	15	Compute Security
	16	Vulnerability & Patch Management
	17	Asset and Configuration Management
	18	Identity and Access Management
	19	Data Protection
	20	Secure System Development

[1] Security Control Framework has been developed using a number of industry standards



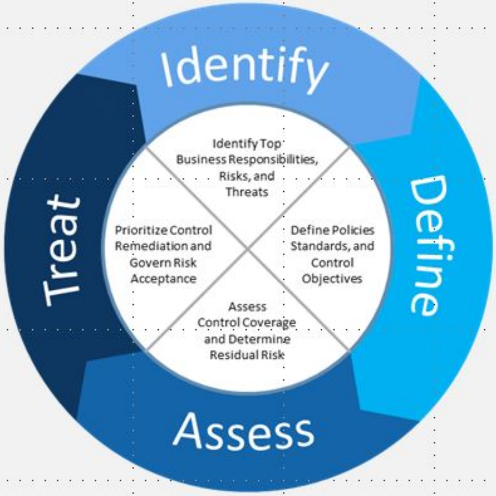
Risk Details - Assessed

Avg Impact	3.8
Max Impact	5.0
Min Impact	3.0
Avg Likelihood	4.3
Max Likelihood	5.0
Min Likelihood	2.0

Risk Framework

Current Goal

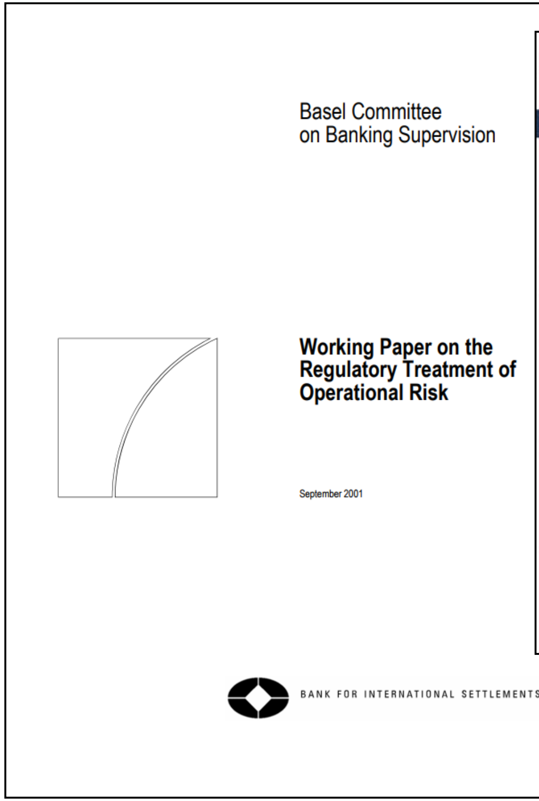
Develop an enterprise risk picture that will help identify and prioritize initiatives to drive down risk across Bridgewater (i.e. what controls do we invest in)


Identify
Define
Assess
Treat
Identify Top Business Responsibilities, Risks, and Threats
Define Policies Standards, and Control Objectives
Assess Control Coverage and Determine Residual Risk
Prioritize Control Remediation and Govern Risk Acceptance

Current Scope

Enterprise Risk Domains[1]	Operational Risk Domains[2]
Strategic Risk	Technology Risk
Reputational Risk	Security
Financial Risk	Business Continuity
Operational Risk	Third Party Risk
Liquidity Risk	Internal/External Fraud
Market Risk	Data Privacy Risk
Capital Risk	Processing Risk
Credit Risk	Human Capital Risk
Legal / Comp. Risk	Project Risk

Risk Domains

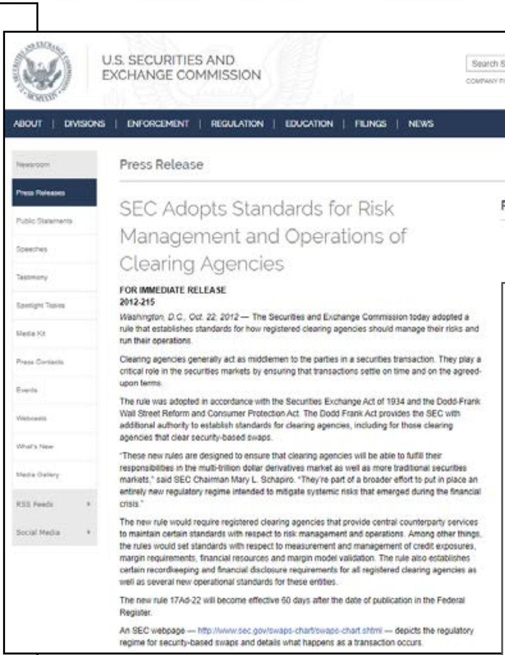


Basel Committee
on Banking Supervision

Working Paper on the Regulatory Treatment of Operational Risk

September 2001

BANK FOR INTERNATIONAL SETTLEMENTS



Press Release

SEC Adopts Standards for Risk Management and Operations of Clearing Agencies

Related Materials

- Final Rule: Clearing Agency Standards
- Fact Sheet

FOR IMMEDIATE RELEASE
2012-215

Washington, D.C., Oct. 22, 2012 — The Securities and Exchange Commission today adopted a rule that establishes standards for how registered clearing agencies should manage their risks and run their operations.

Clearing agencies generally act as middlemen to the parties in a securities transaction. They play a critical role in the securities markets by ensuring that transactions settle on time and on the agreed-upon terms.

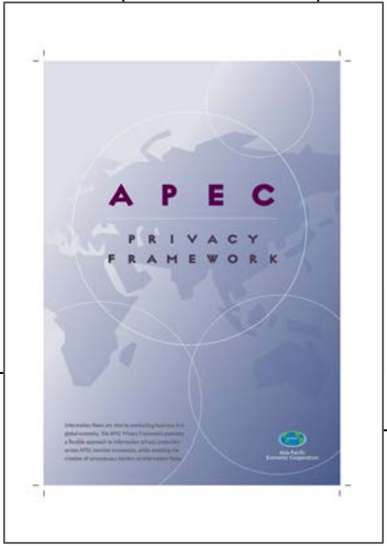
The rule was adopted in accordance with the Securities Exchange Act of 1934 and the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Dodd Frank Act provides the SEC with additional authority to establish standards for clearing agencies, including for those clearing agencies that clear security-based swaps.

"These new rules are designed to ensure that clearing agencies will be able to fulfill their responsibilities in the multi-trillion dollar derivatives market as well as more traditional securities markets," said SEC Chairman Mary L. Schapiro. "They're part of a broader effort to put in place an entirely new regulatory regime intended to mitigate systemic risks that emerged during the financial crisis."

The new rule would require registered clearing agencies that provide central counterparty services to maintain certain standards with respect to risk management and operations. Among other things, the rules would set standards with respect to measurement and management of credit exposures, margin requirements, financial resources and margin model validation. The rule also establishes certain recordkeeping and financial disclosure requirements for all registered clearing agencies as well as several new operational standards for these entities.

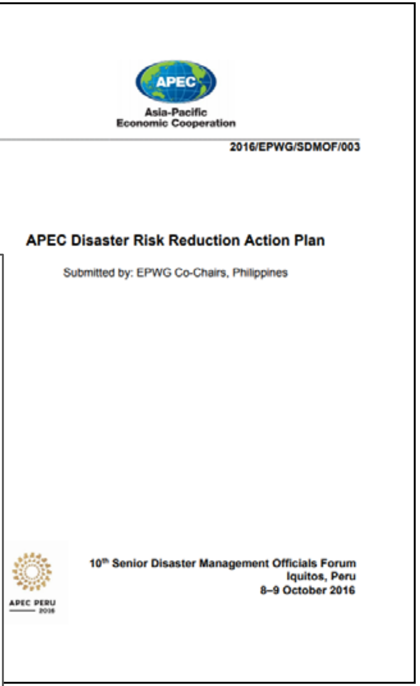
The new rule 17Ad-22 will become effective 60 days after the date of publication in the Federal Register.

An SEC webpage — http://www.sec.gov/swaps-chart/swaps-chart.shtml — depicts the regulatory regime for security-based swaps and details what happens as a transaction occurs.



APEC
PRIVACY
FRAMEWORK

Information flows are vital to conducting business in a global economy. The APEC Privacy Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.



APEC
Asia-Pacific
Economic Cooperation

2016/EPWG/SDMOF/003

APEC Disaster Risk Reduction Action Plan

Submitted by: EPWG Co-Chairs, Philippines

10th Senior Disaster Management Officials Forum
Iquitos, Peru
8–9 October 2016

Risk Framework

Risk Identification

1 External party takes down systems / causes denial of service

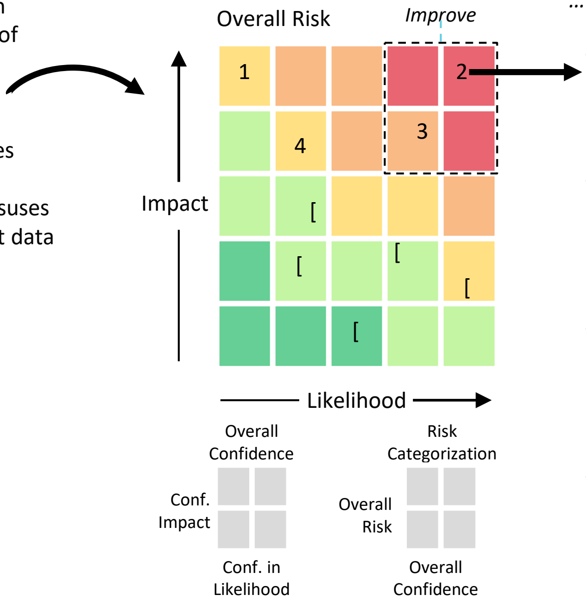
2 External party steals / exfiltrates pending trades

3 Authorized Employee misuses knowledge of Top Secret data

4 Employee leaks client information

Risk Assessment

Analyze + classify those risk scenarios …



Control Mapping

Understand controls needed to address risk …

Kill Chain	Threat	Controls
Recon	Social Engineering	• Security Training and Awareness
Infiltrate	Malware / Phishing	• Endpoint Prot. • Vuln/Patch Mgmt
Gain Access	Credential Theft	• MFA • Key Mgmt
Execute	Data Exfiltration	• DLP • Web Proxies

Prioritize and Define Initiatives

Build/improve controls that drive down risk

Prioritize Perceived Risks and Control Gaps

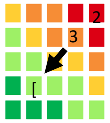
2 External party hacks BW and steals / exfiltrates TS data

3 Authorized Employee steals / misuses their knowledge …

1 External party hacks and takes down BW systems / denial…

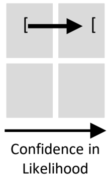
4 Employee physically steals TS data

Initiatives that Address Risks



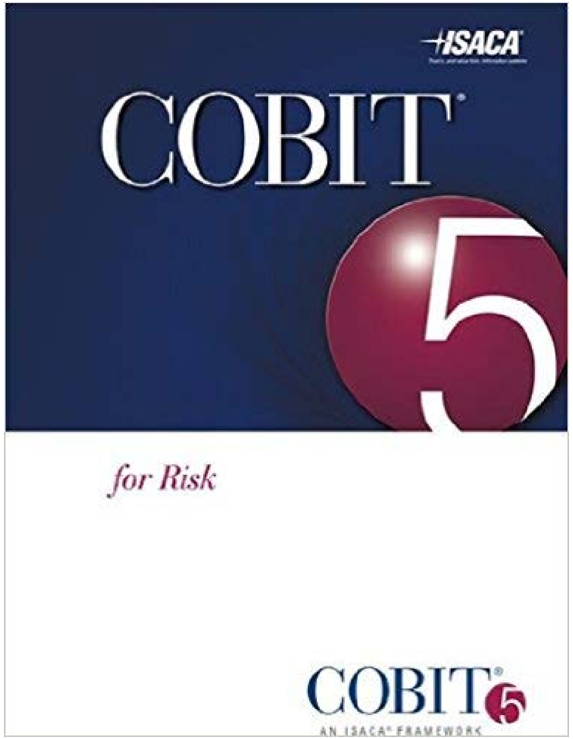
Project A and B
These projects are designed to reduce risk 2 and 3 respectively

Initiatives that Increase Confidence



Project C
This project is designed to increase the confidence for a potentially high impact risk

Risk Frameworks– EXTERNAL SOURCES


ISACA

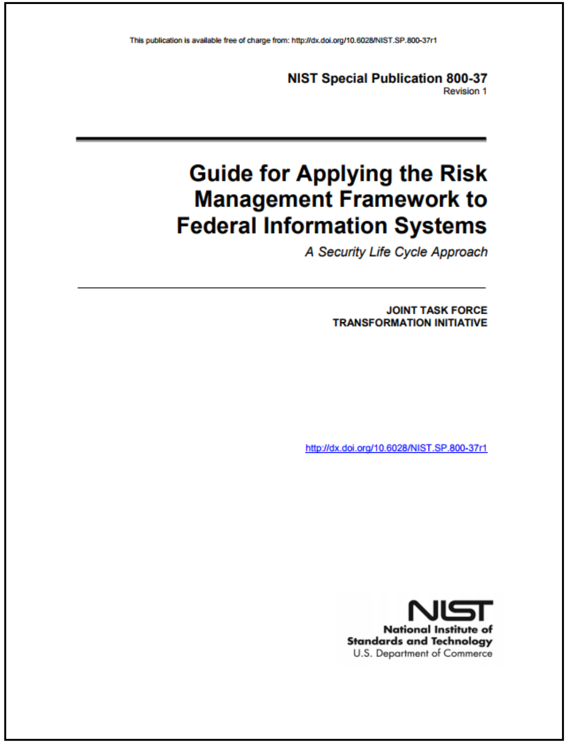
COBIT®

5

for Risk

COBIT® 5

AN ISACA® FRAMEWORK


This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-37r1

NIST Special Publication 800-37
Revision 1

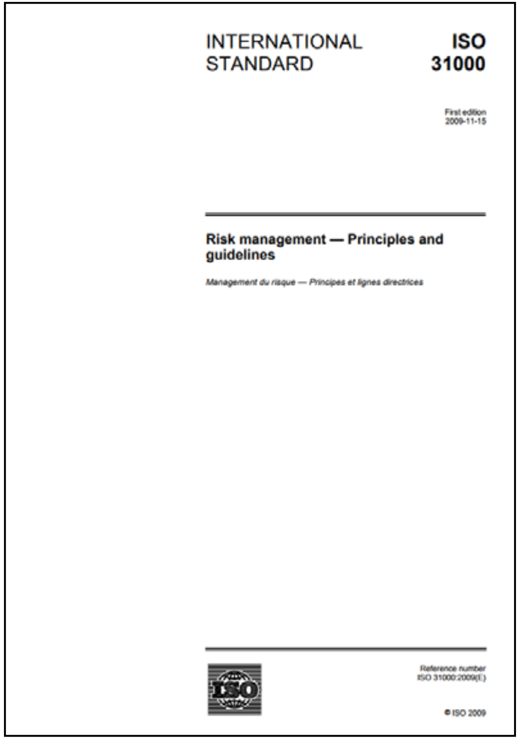
Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-37r1

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


INTERNATIONAL STANDARD

ISO 31000

First edition
2009-11-15

Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number
ISO 31000:2009(E)

© ISO 2009

Business buy-in/Support

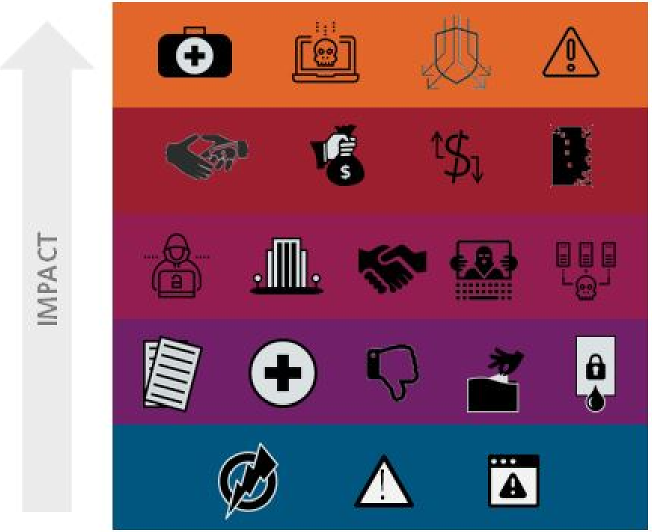
- Enterprise Risk Assessments

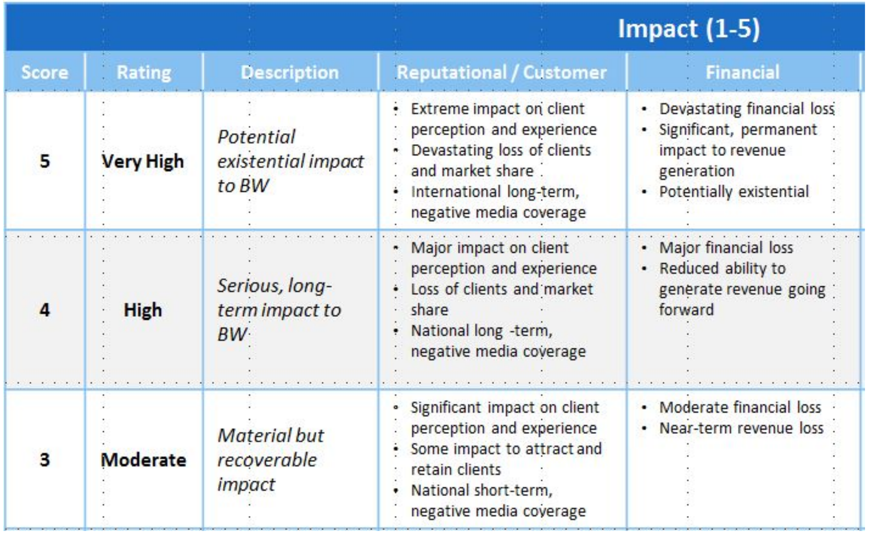
1. Captured department risks with Security SME’s.
2. Conducted Risk Workshops with DH.

<u>Key to Success</u>

- Get buy-in from the business
- Keep it simple and interactive
- Establish clear rules of the road
- Cut off debate

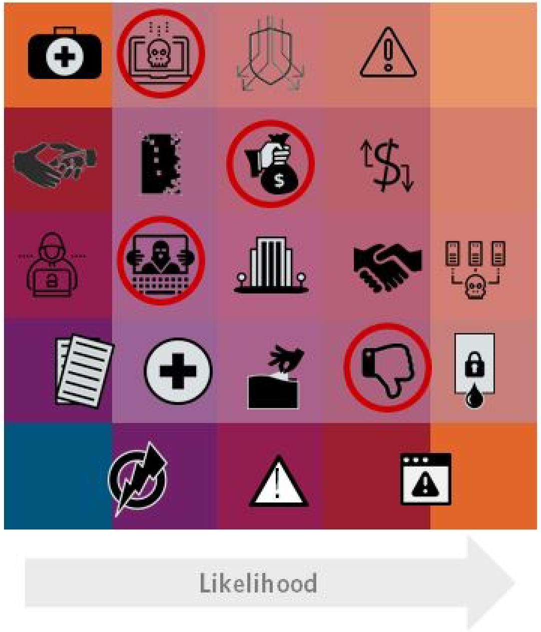
Enterprise Risk Assessments

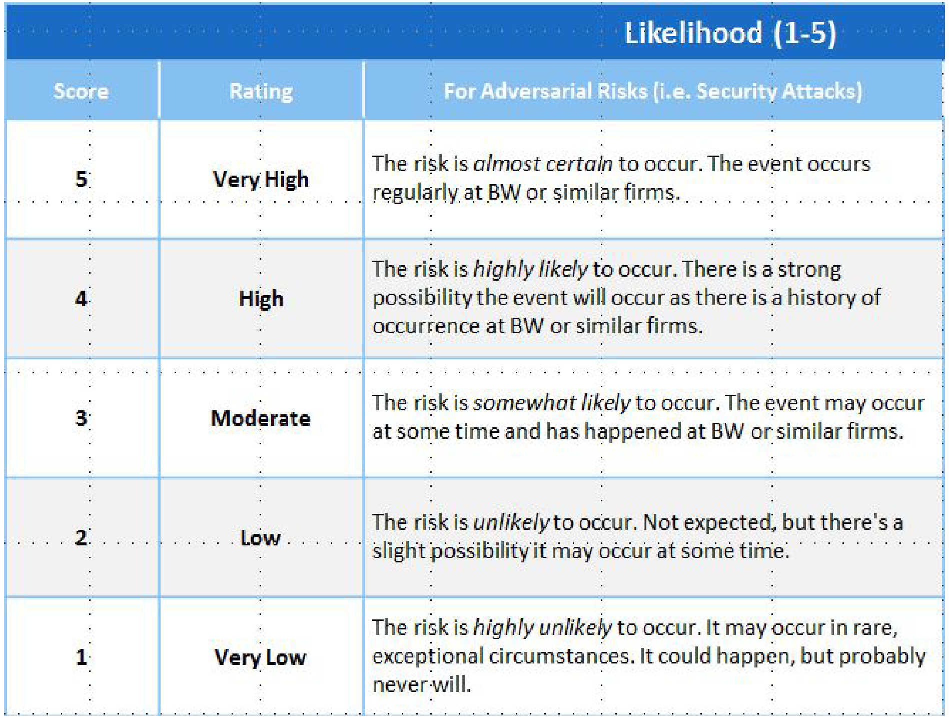




		Impact (1-5)		
Score	**Rating**	**Description**	**Reputational / Customer**	**Financial**
5	**Very High**	*Potential existential impact to BW*	• Extreme impact on client perception and experience • Devastating loss of clients and market share • International long-term, negative media coverage	• Devastating financial loss • Significant, permanent impact to revenue generation • Potentially existential
4	**High**	*Serious, long-term impact to BW*	• Major impact on client perception and experience • Loss of clients and market share • National long -term, negative media coverage	• Major financial loss • Reduced ability to generate revenue going forward
3	**Moderate**	*Material but recoverable impact*	• Significant impact on client perception and experience • Some impact to attract and retain clients • National short-term, negative media coverage	• Moderate financial loss • Near-term revenue loss

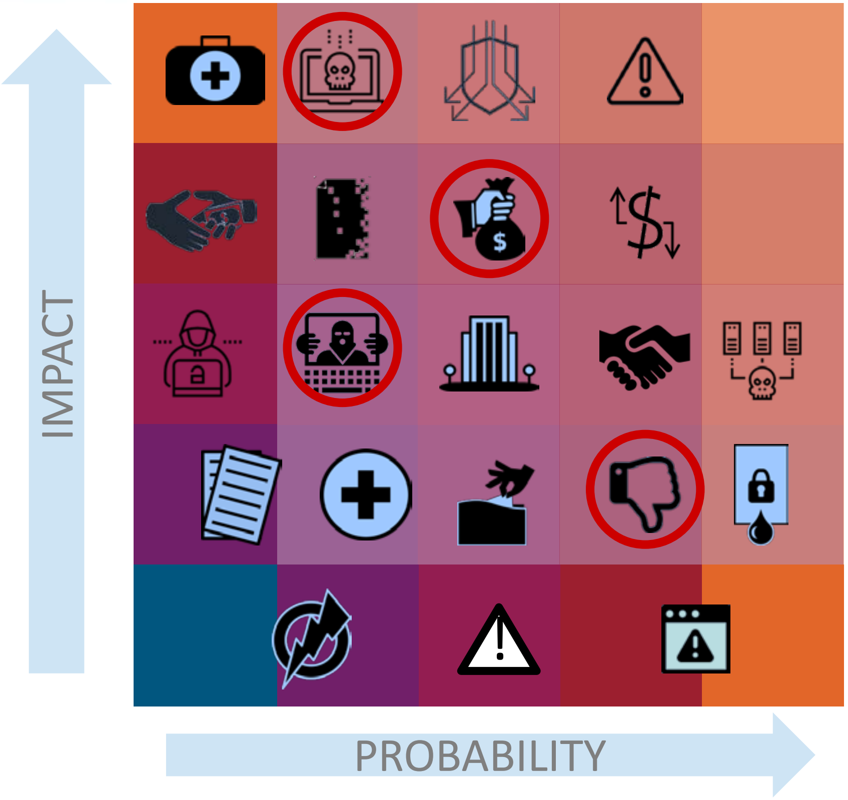
Enterprise Risk Assessment

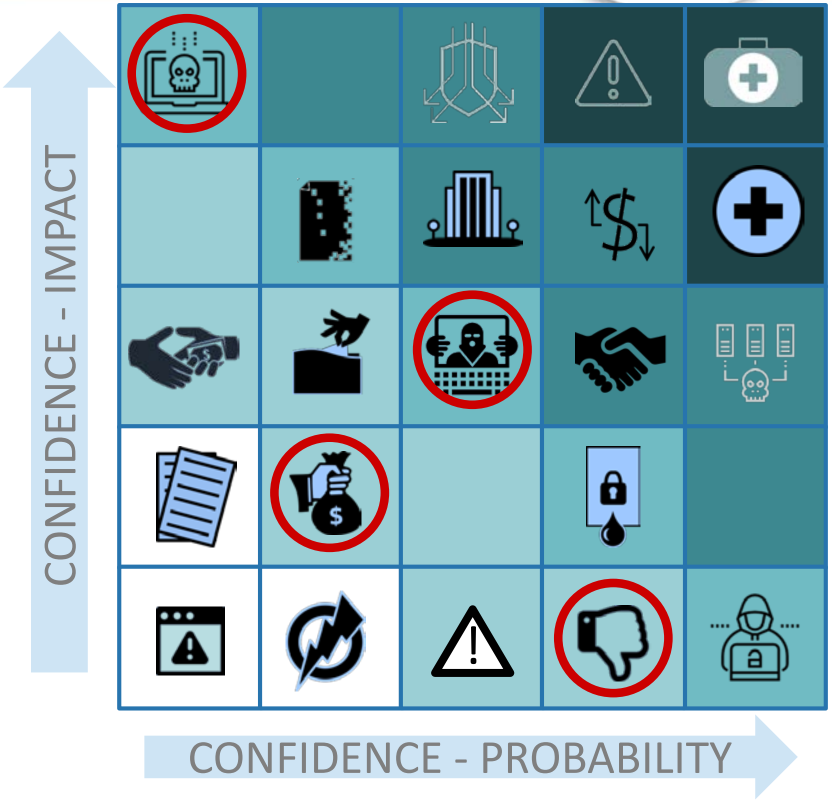




Likelihood (1-5)		
Score	Rating	For Adversarial Risks (i.e. Security Attacks)
5	Very High	The risk is *almost certain* to occur. The event occurs regularly at BW or similar firms.
4	High	The risk is *highly likely* to occur. There is a strong possibility the event will occur as there is a history of occurrence at BW or similar firms.
3	Moderate	The risk is *somewhat likely* to occur. The event may occur at some time and has happened at BW or similar firms.
2	Low	The risk is *unlikely* to occur. Not expected, but there's a slight possibility it may occur at some time.
1	Very Low	The risk is *highly unlikely* to occur. It may occur in rare, exceptional circumstances. It could happen, but probably never will.

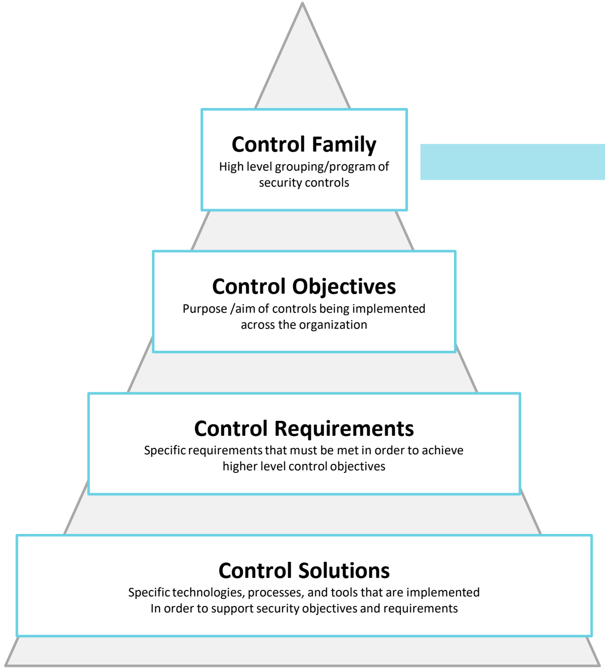
Risk Framework – Confidence





Security Control Framework

Customized taxonomy used to categorize our controls



Control Family
High level grouping/program of security controls

Control Objectives
Purpose /aim of controls being implemented across the organization

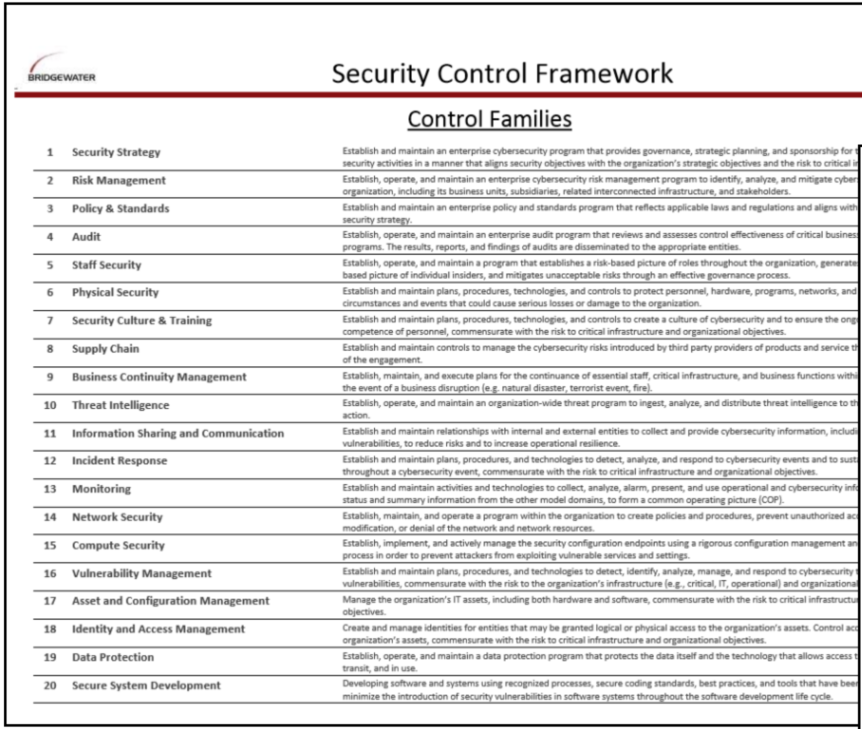
Control Requirements
Specific requirements that must be met in order to achieve higher level control objectives

Control Solutions
Specific technologies, processes, and tools that are implemented In order to support security objectives and requirements

	ID	Control Family[1]
Mgmt	1	Security Strategy
	2	Risk Management
	3	Policy & Standards
	4	Audit
Operational	5	Staff Security
	6	Physical Security
	7	Security Culture & Training
	8	Supply Chain
	9	Business Continuity Management
	10	Threat Intelligence
	11	Information Sharing and Communications
	12	Incident Response
Technology	13	Monitoring
	14	Network Security
	15	Compute Security
	16	Vulnerability & Patch Management
	17	Asset and Configuration Management
	18	Identity and Access Management
	19	Data Protection
	20	Secure System Development

1. *Security Control Framework has been developed using a number of industry standards and references for security controls, including: NIST, Cobit, ISO, and CIS/SANS.*

Control Frameworks– SCF / DYNAMIC DOT

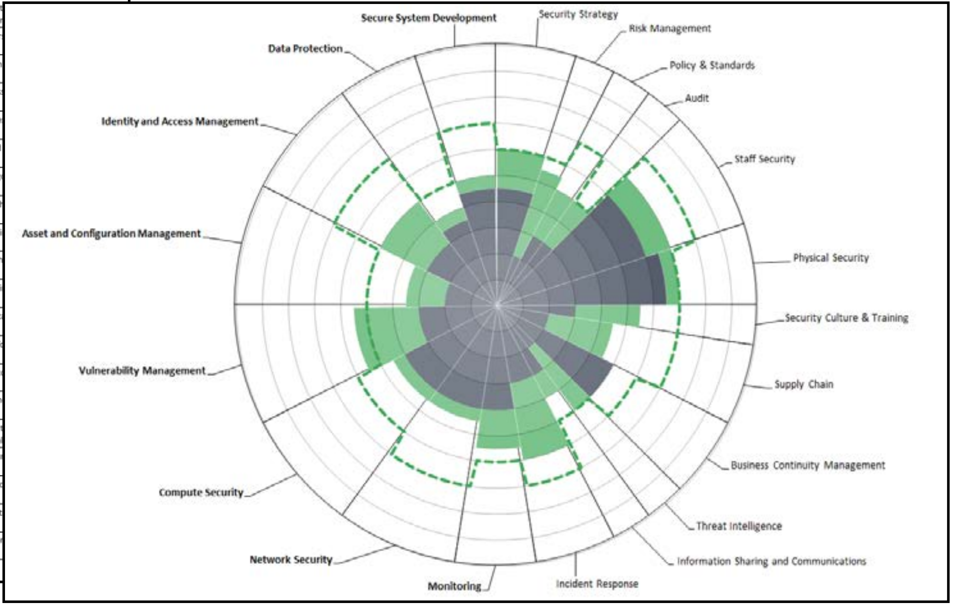


BRIDGEWATER

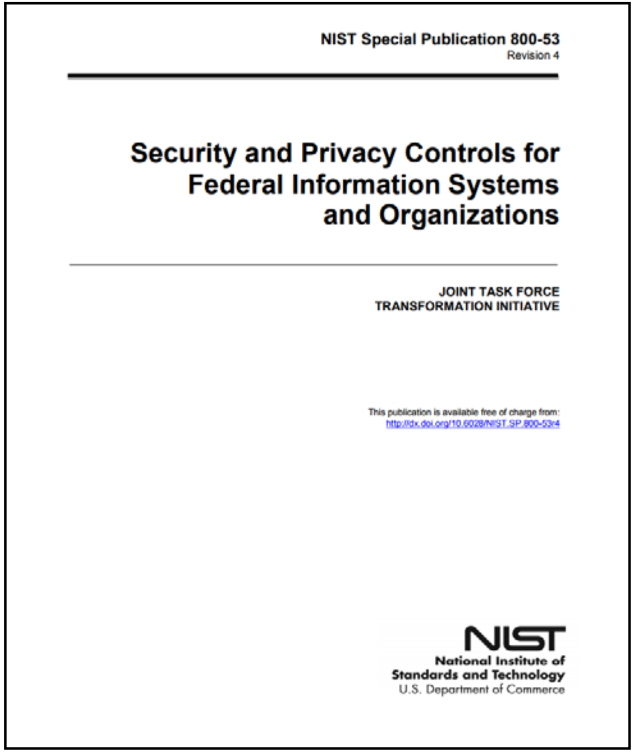
Security Control Framework

Control Families

1	Security Strategy	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for t security activities in a manner that aligns security objectives with the organization's strategic objectives and the risk to critical i
2	Risk Management	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cyber organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
3	Policy & Standards	Establish and maintain an enterprise policy and standards program that reflects applicable laws and regulations and aligns with security strategy.
4	Audit	Establish, operate, and maintain an enterprise audit program that reviews and assesses control effectiveness of critical busines programs. The results, reports, and findings of audits are disseminated to the appropriate entities.
5	Staff Security	Establish, operate, and maintain a program that establishes a risk-based picture of roles throughout the organization, generate based picture of individual insiders, and mitigates unacceptable risks through an effective governance process.
6	Physical Security	Establish and maintain plans, procedures, technologies, and controls to protect personnel, hardware, programs, networks, and circumstances and events that could cause serious losses or damage to the organization.
7	Security Culture & Training	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ong competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.
8	Supply Chain	Establish and maintain controls to manage the cybersecurity risks introduced by third party providers of products and service th of the engagement.
9	Business Continuity Management	Establish, maintain, and execute plans for the continuance of essential staff, critical infrastructure, and business functions withi the event of a business disruption (e.g. natural disaster, terrorist event, fire).
10	Threat Intelligence	Establish, operate, and maintain an organization-wide threat program to ingest, analyze, and distribute threat intelligence to th action.
11	Information Sharing and Communication	Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, includi vulnerabilities, to reduce risks and to increase operational resilience.
12	Incident Response	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sust throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.
13	Monitoring	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity inf status and summary information from the other model domains, to form a common operating picture (COP).
14	Network Security	Establish, maintain, and operate a program within the organization to create policies and procedures, prevent unauthorized ac modification, or denial of the network and network resources.
15	Compute Security	Establish, implement, and actively manage the security configuration endpoints using a rigorous configuration management an process in order to prevent attackers from exploiting vulnerable services and settings.
16	Vulnerability Management	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity t vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational
17	Asset and Configuration Management	Manage the organization's IT assets, including both hardware and software, commensurate with the risk to critical infrastructu objectives.
18	Identity and Access Management	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control acc organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.
19	Data Protection	Establish, operate, and maintain a data protection program that protects the data itself and the technology that allows access t transit, and in use.
20	Secure System Development	Developing software and systems using recognized processes, secure coding standards, best practices, and tools that have bee minimize the introduction of security vulnerabilities in software systems throughout the software development life cycle.



Control Frameworks



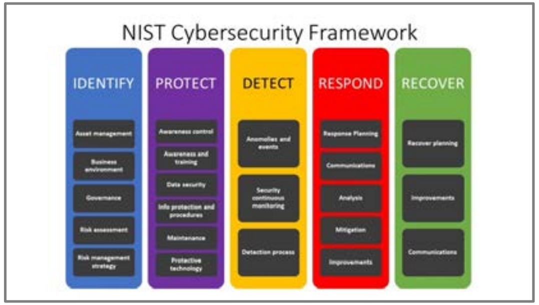
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

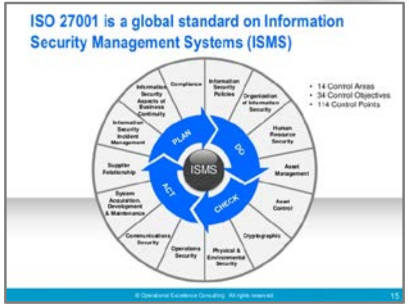
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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



NIST Cybersecurity Framework

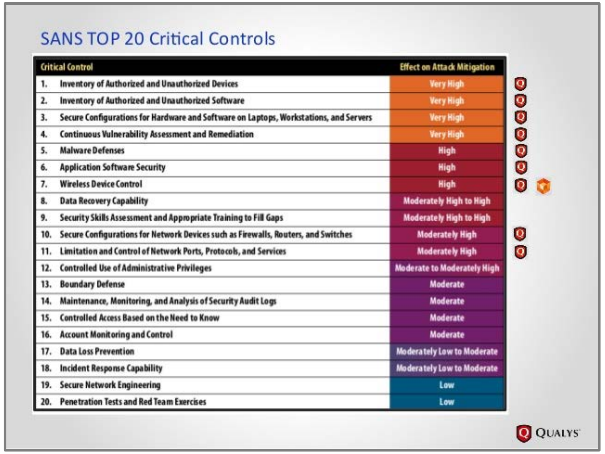


ISO 27001 is a global standard on Information Security Management Systems (ISMS)

- 14 Control Areas
- 34 Control Objectives
- 114 Control Points

Compliance
Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Asset Control
Cryptographic
Physical & Environmental Security
Operations Security
Communications Security
System Acquisition, Development & Maintenance
Supplier Relationship
Information Security Incident Management
Information Security Aspects of Business Continuity
PLAN
DO
CHECK
ACT
ISMS

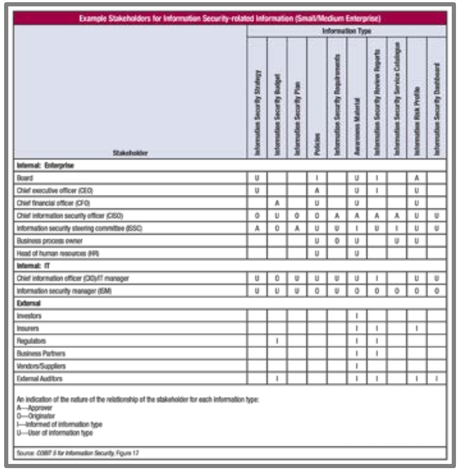
© Operational Excellence Consulting. All rights reserved. 15



SANS TOP 20 Critical Controls

Critical Control	Effect on Attack Mitigation
1. Inventory of Authorized and Unauthorized Devices	Very High
2. Inventory of Authorized and Unauthorized Software	Very High
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4. Continuous Vulnerability Assessment and Remediation	Very High
5. Malware Defenses	High
6. Application Software Security	High
7. Wireless Device Control	High
8. Data Recovery Capability	Moderately High to High
9. Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12. Controlled Use of Administrative Privileges	Moderate to Moderately High
13. Boundary Defense	Moderate
14. Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15. Controlled Access Based on the Need to Know	Moderate
16. Account Monitoring and Control	Moderate
17. Data Loss Prevention	Moderately Low to Moderate
18. Incident Response Capability	Moderately Low to Moderate
19. Secure Network Engineering	Low
20. Penetration Tests and Red Team Exercises	Low

QUALYS



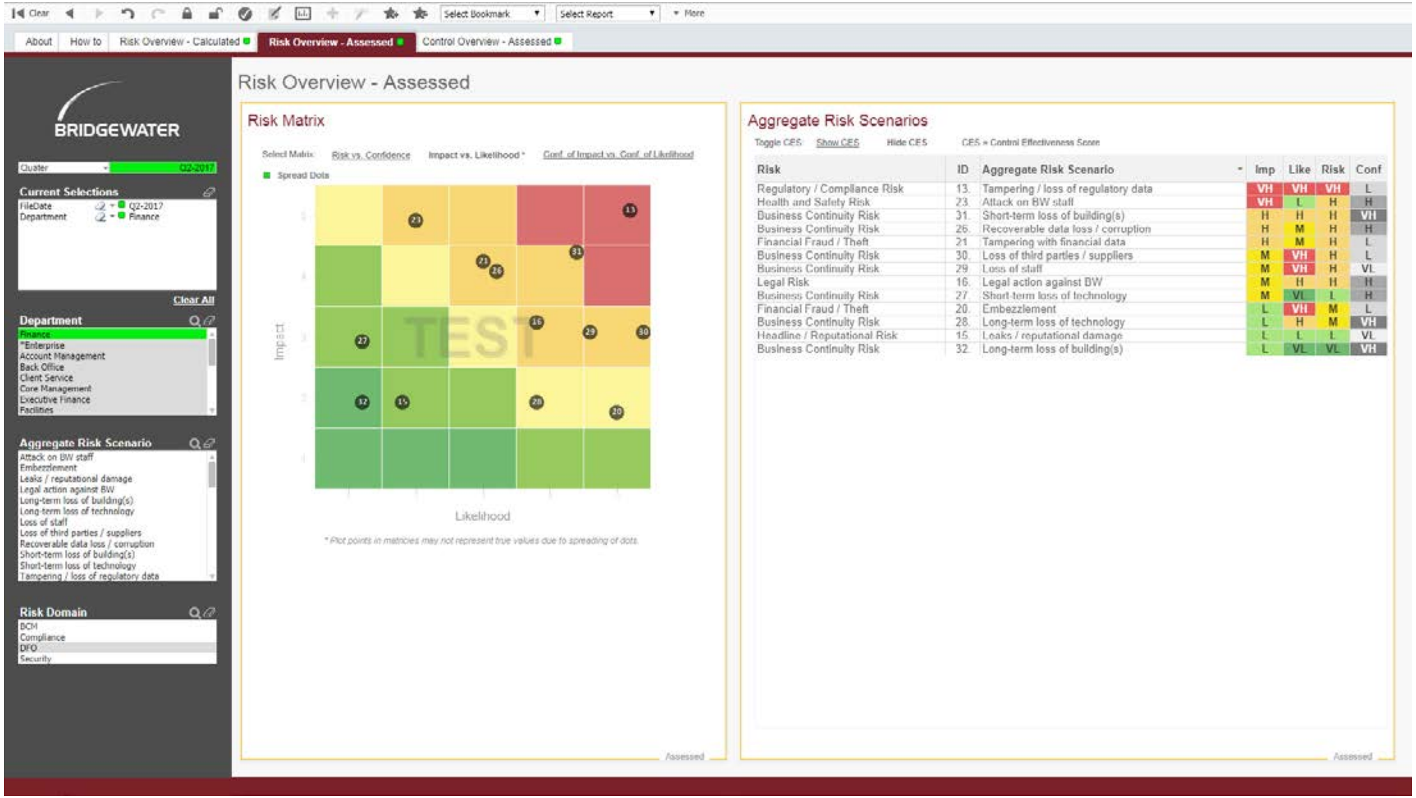
Example Stakeholders for Information Security-related Information (Small/Medium Enterprise)

Stakeholder	Information Security Strategy	Information Security Budget	Information Security Plan	Policies	Information Security Requirements	Awareness Material	Information Security Review Reports	Information Security Service Catalogue	Information Risk Profile	Information Security Dashboard
Internal: Enterprise										
Board	U			I		U	I		A	
Chief executive officer (CEO)	U			A		U	I		U	
Chief financial officer (CFO)		A		U		U			U	
Chief information security officer (CISO)	O	U	O	O	A	A	A	A	U	U
Information security steering committee (ISSC)	A	O	A	U	U	I	U	I	U	U
Business process owner				U	O	U		U	U	
Head of human resources (HR)				U		U				
Internal: IT										
Chief information officer (CIO)/IT manager	U	O	U	U	U	U	I		U	U
Information security manager (ISM)	U	U	U	O	U	O	O	O	O	O
External										
Investors						I				
Insurers						I	I		I	
Regulators		I				I	I			
Business Partners						I	I			
Vendors/Suppliers						I				
External Auditors		I				I	I		I	I

An indication of the nature of the relationship of the stakeholder for each information type:
A—Approver
O—Originator
I—Informed of information type
U—User of information type

Source: *COBIT 5 for Information Security*, Figure 17

Tooling



Risk Overview - Assessed

Quater Q2-2017

Current Selections

FileDate Q2-2017
Department Finance

Clear All

Department

Finance
*Enterprise
Account Management
Back Office
Client Service
Core Management
Executive Finance
Facilities

Aggregate Risk Scenario

Attack on BW staff
Embezzlement
Leaks / reputational damage
Legal action against BW
Long-term loss of building(s)
Long-term loss of technology
Loss of staff
Loss of third parties / suppliers
Recoverable data loss / corruption
Short-term loss of building(s)
Short-term loss of technology
Tampering / loss of regulatory data

Risk Domain

BCM
Compliance
DFO
Security

Risk Matrix

Select Matrix: Risk vs. Confidence Impact vs. Likelihood * Conf. of Impact vs. Conf. of Likelihood

🟩 Spread Dots

* Plot points in matrices may not represent true values due to spreading of dots.

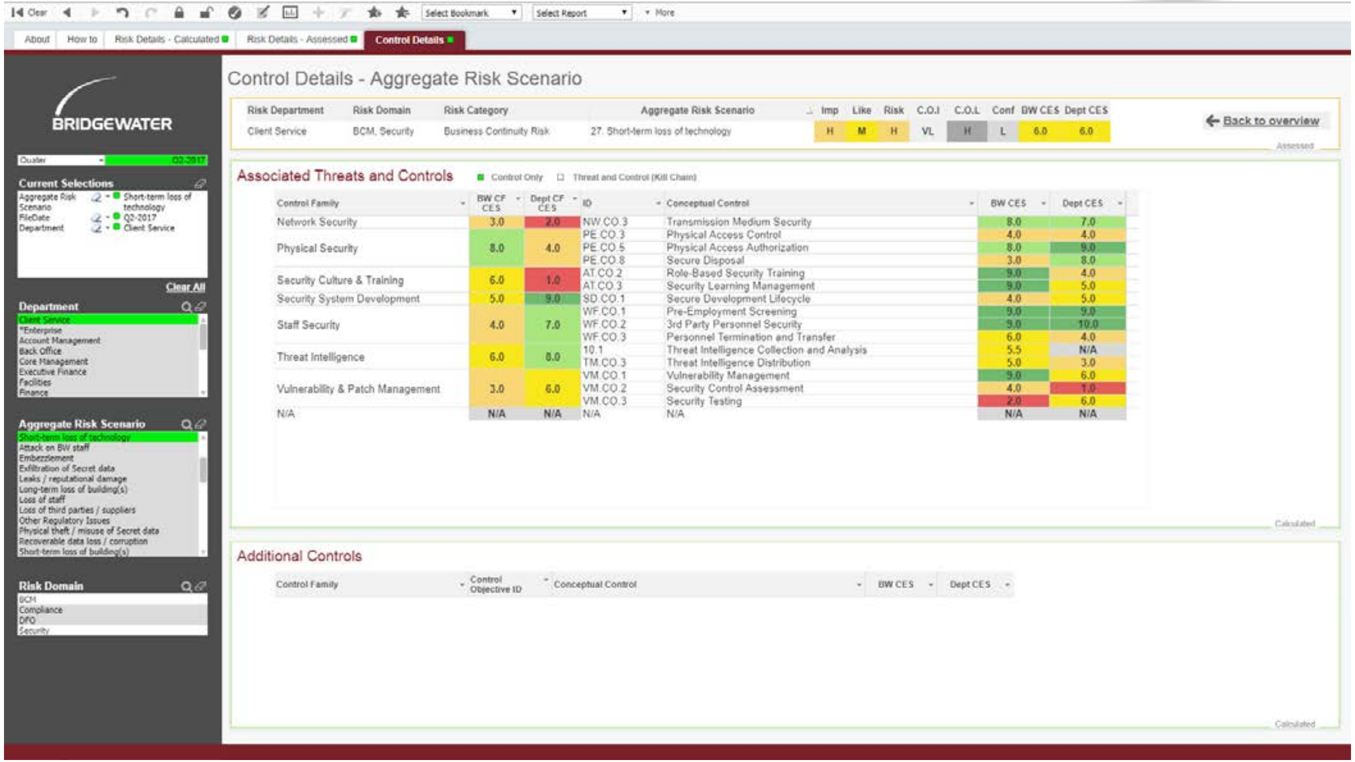
Aggregate Risk Scenarios

Toggle CES Show CES Hide CES CES = Control Effectiveness Score

Risk	ID	Aggregate Risk Scenario	Imp	Like	Risk	Conf
Regulatory / Compliance Risk	13.	Tampering / loss of regulatory data	VH	VH	VH	L
Health and Safety Risk	23.	Attack on BW staff	VH	L	H	H
Business Continuity Risk	31.	Short-term loss of building(s)	H	H	H	VH
Business Continuity Risk	26.	Recoverable data loss / corruption	H	M	H	H
Financial Fraud / Theft	21.	Tampering with financial data	H	M	H	L
Business Continuity Risk	30.	Loss of third parties / suppliers	M	VH	H	L
Business Continuity Risk	29.	Loss of staff	M	VH	H	VL
Legal Risk	16.	Legal action against BW	M	H	H	H
Business Continuity Risk	27.	Short-term loss of technology	M	VL	L	H
Financial Fraud / Theft	20.	Embezzlement	L	VH	M	L
Business Continuity Risk	28.	Long-term loss of technology	L	H	M	VH
Headline / Reputational Risk	15.	Leaks / reputational damage	L	L	L	VL
Business Continuity Risk	32.	Long-term loss of building(s)	L	VL	VL	VH

Tool – Risk Library and Dashboard

Control Mapping and Ratings



Quater: Q2-2017

Current Selections

Aggregate Risk Scenario	Short-term loss of technology
FileDate	Q2-2017
Department	Client Service

Clear All

Department

- Client Service
- *Enterprise
- Account Management
- Back Office
- Core Management
- Executive Finance
- Facilities
- Finance

Aggregate Risk Scenario

- Short-term loss of technology
- Attack on BW staff
- Embezzlement
- Exfiltration of Secret data
- Leaks / reputational damage
- Long-term loss of building(s)
- Loss of staff
- Loss of third parties / suppliers
- Other Regulatory Issues
- Physical theft / misuse of Secret data
- Recoverable data loss / corruption
- Short-term loss of building(s)

Risk Domain

- BCM
- Compliance
- DFO
- Security

Control Details - Aggregate Risk Scenario

Risk Department	Risk Domain	Risk Category	Aggregate Risk Scenario	Imp	Like	Risk	C.O.I	C.O.L	Conf	BW CES	Dept CES
Client Service	BCM, Security	Business Continuity Risk	27. Short-term loss of technology	H	M	H	VL	H	L	6.0	6.0

Associated Threats and Controls

■ Control Only ☐ Threat and Control (Kill Chain)

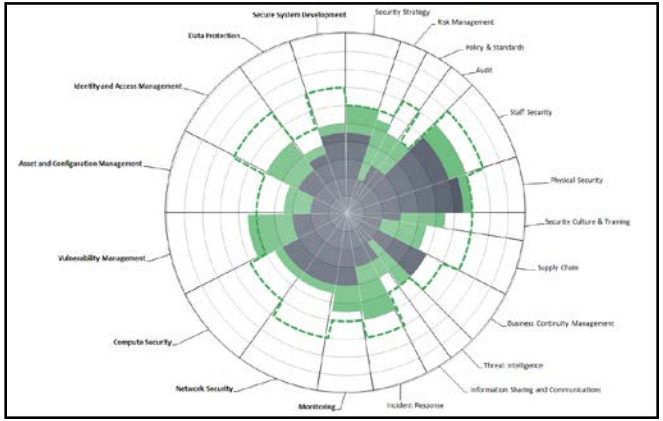
Control Family	BW CF CES	Dept CF CES	ID	Conceptual Control	BW CES	Dept CES
Network Security	3.0	2.0	NW.CO.3	Transmission Medium Security	8.0	7.0
Physical Security	8.0	4.0	PE.CO.3	Physical Access Control	4.0	4.0
			PE.CO.5	Physical Access Authorization	8.0	9.0
			PE.CO.8	Secure Disposal	3.0	8.0
Security Culture & Training	6.0	1.0	AT.CO.2	Role-Based Security Training	9.0	4.0
			AT.CO.3	Security Learning Management	9.0	5.0
Security System Development	5.0	9.0	SD.CO.1	Secure Development Lifecycle	4.0	5.0
Staff Security	4.0	7.0	WF.CO.1	Pre-Employment Screening	9.0	9.0
			WF.CO.2	3rd Party Personnel Security	9.0	10.0
			WF.CO.3	Personnel Termination and Transfer	6.0	4.0
Threat Intelligence	6.0	8.0	10.1	Threat Intelligence Collection and Analysis	5.5	N/A
			TM.CO.3	Threat Intelligence Distribution	5.0	3.0
Vulnerability & Patch Management	3.0	6.0	VM.CO.1	Vulnerability Management	9.0	6.0
			VM.CO.2	Security Control Assessment	4.0	1.0
			VM.CO.3	Security Testing	2.0	6.0
N/A	N/A	N/A	N/A	N/A	N/A	N/A

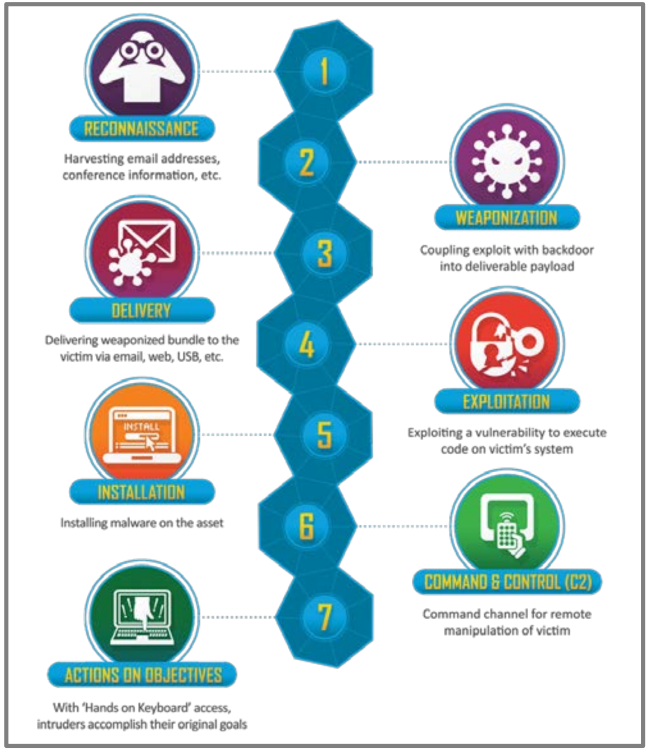
Additional Controls

Control Family	Control Objective ID	Conceptual Control	BW CES	Dept CES

Control Mapping – Kill Chain analysis

Risk → Threat Vectors → Assets





RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

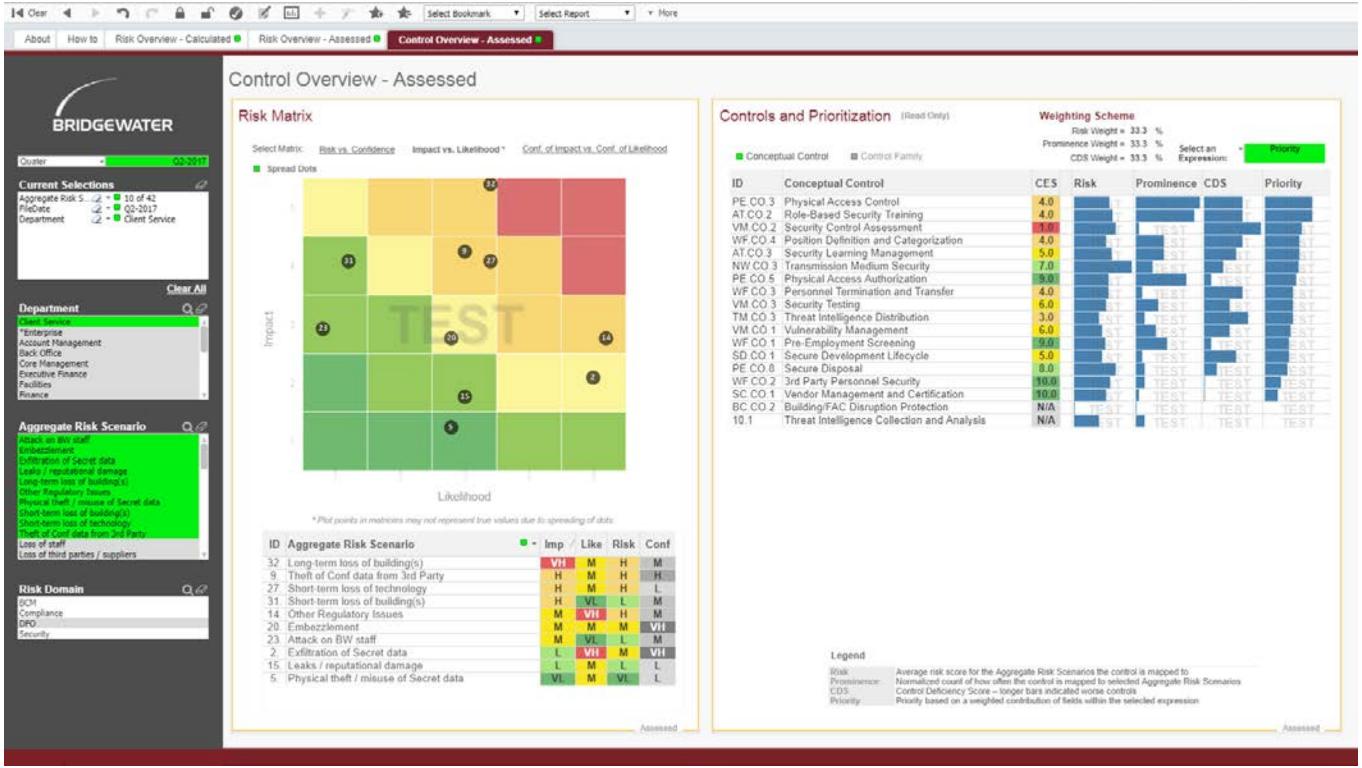
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Tool – Risk Library and Dashboard

Dynamic Control Prioritization



Quater: Q2-2017

Current Selections

Aggregate Risk S...	10 of 42
FileDate	Q2-2017
Department	Client Service

Clear All

Department

- Client Service
- *Enterprise
- Account Management
- Back Office
- Core Management
- Executive Finance
- Facilities
- Finance

Aggregate Risk Scenario

- Attack on BW staff
- Embezzlement
- Exfiltration of Secret data
- Leaks / reputational damage
- Long-term loss of building(s)
- Other Regulatory Issues
- Physical theft / misuse of Secret data
- Short-term loss of building(s)
- Short-term loss of technology
- Theft of Conf data from 3rd Party
- Loss of staff
- Loss of third parties / suppliers

Risk Domain

- BCM
- Compliance
- DFO
- Security

Control Overview - Assessed

Risk Matrix

Select Matrix: Risk vs. Confidence | **Impact vs. Likelihood** * | Conf. of Impact vs. Conf. of Likelihood

🟩 Spread Dots

* Plot points in matrices may not represent true values due to spreading of dots

ID	Aggregate Risk Scenario	Imp	Like	Risk	Conf
32	Long-term loss of building(s)	VH	M	H	M
9	Theft of Conf data from 3rd Party	H	M	H	H
27	Short-term loss of technology	H	M	H	L
31	Short-term loss of building(s)	H	VL	L	M
14	Other Regulatory Issues	M	VH	H	M
20	Embezzlement	M	M	M	VH
23	Attack on BW staff	M	VL	L	M
2	Exfiltration of Secret data	L	VH	M	VH
15	Leaks / reputational damage	L	M	L	L
5	Physical theft / misuse of Secret data	VL	M	VL	L

Assessed

Controls and Prioritization (Read Only)

Weighting Scheme

Risk Weight = 33.3 %
Prominence Weight = 33.3 %
CDS Weight = 33.3 %

Select an Expression: Priority

🟩 Conceptual Control ▨ Control Family

ID	Conceptual Control	CES	Risk	Prominence	CDS	Priority
PE.CO.3	Physical Access Control	4.0				
AT.CO.2	Role-Based Security Training	4.0				
VM.CO.2	Security Control Assessment	1.0				
WF.CO.4	Position Definition and Categorization	4.0				
AT.CO.3	Security Learning Management	5.0				
NW.CO.3	Transmission Medium Security	7.0				
PE.CO.5	Physical Access Authorization	9.0				
WF.CO.3	Personnel Termination and Transfer	4.0				
VM.CO.3	Security Testing	6.0				
TM.CO.3	Threat Intelligence Distribution	3.0				
VM.CO.1	Vulnerability Management	6.0				
WF.CO.1	Pre-Employment Screening	9.0				
SD.CO.1	Secure Development Lifecycle	5.0				
PE.CO.8	Secure Disposal	8.0				
WF.CO.2	3rd Party Personnel Security	10.0				
SC.CO.1	Vendor Management and Certification	10.0				
BC.CO.2	Building/FAC Disruption Protection	N/A				
10.1	Threat Intelligence Collection and Analysis	N/A				

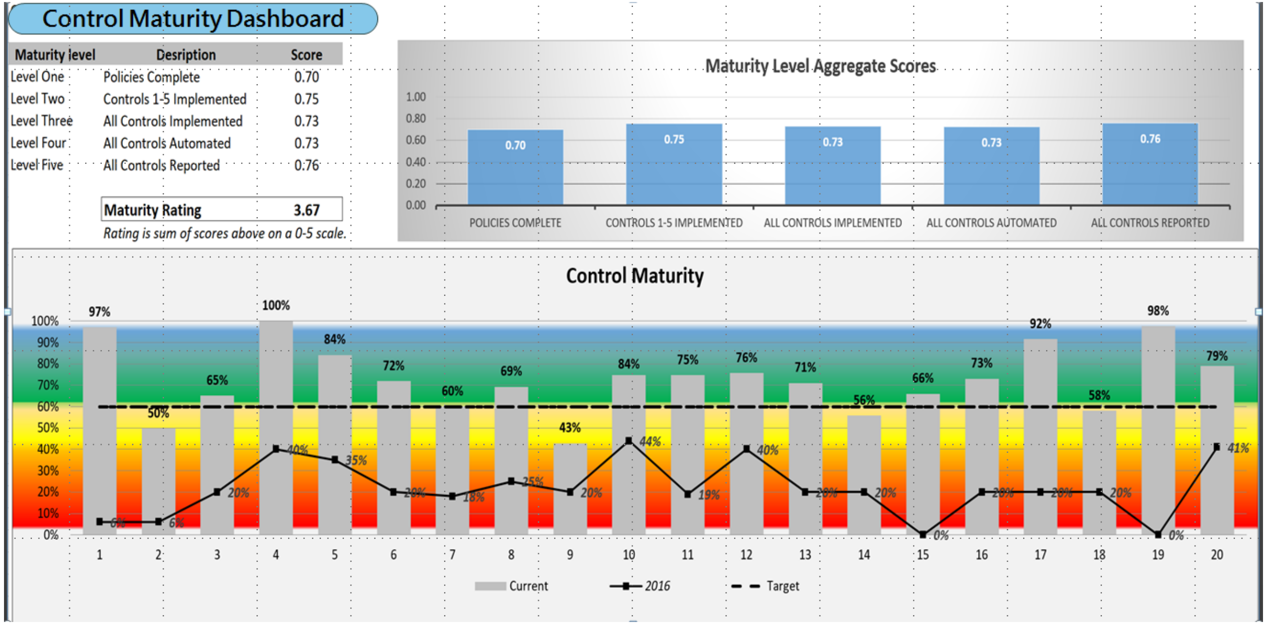
Legend

Risk	Average risk score for the Aggregate Risk Scenarios the control is mapped to
Prominence	Normalized count of how often the control is mapped to selected Aggregate Risk Scenarios
CDS	Control Deficiency Score – longer bars indicated worse controls
Priority	Priority based on a weighted contribution of fields within the selected expression

Assessed

Bank of the Ozarks Risk Management Tooling

https://www.linkedin.com/pulse/cybersecurity-risk-control-maturity-assessment-fricke-cissp-cism/



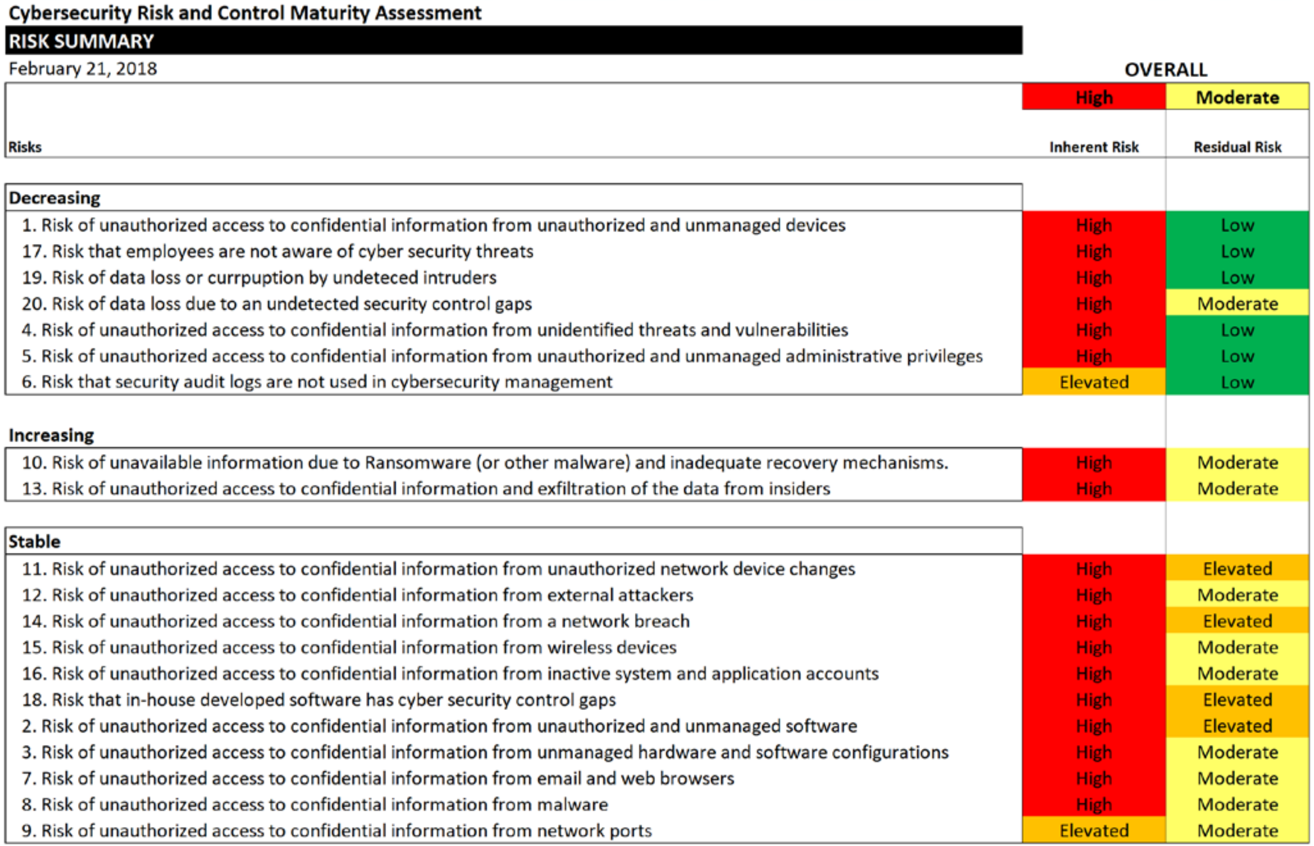
Control Maturity Dashboard

Maturity level	Desription	Score
Level One	Policies Complete	0.70
Level Two	Controls 1-5 Implemented	0.75
Level Three	All Controls Implemented	0.73
Level Four	All Controls Automated	0.73
Level Five	All Controls Reported	0.76

Maturity Rating	3.67

Rating is sum of scores above on a 0-5 scale.

Bank Of Ozarks – Risk Dashboard



Cybersecurity Risk and Control Maturity Assessment

RISK SUMMARY

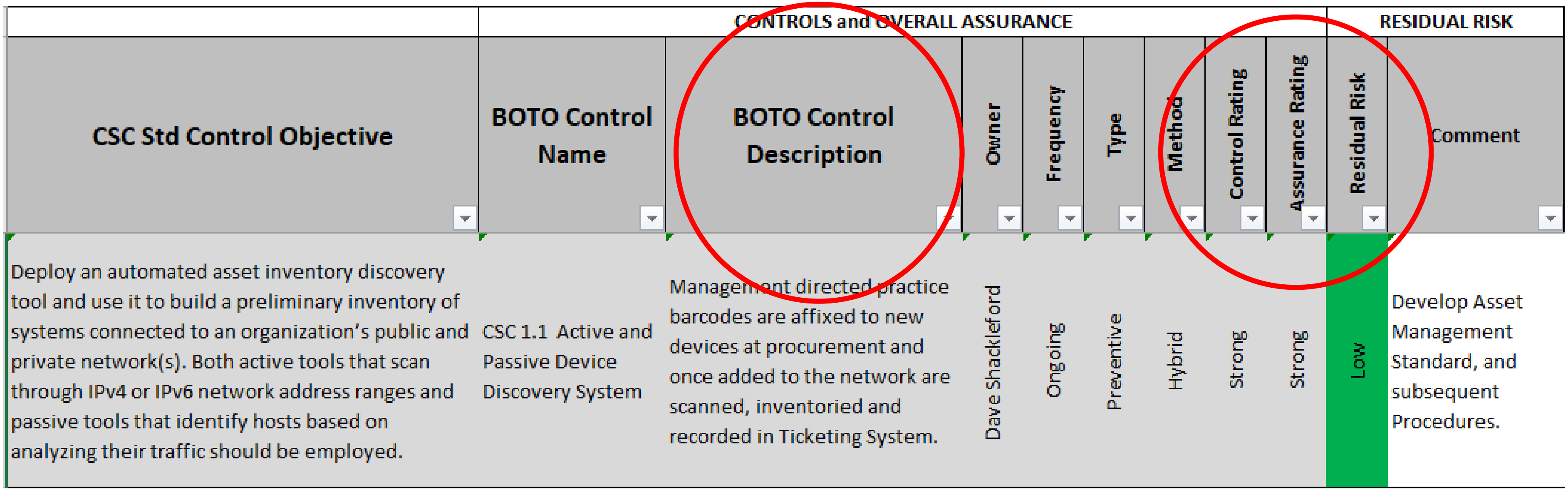
February 21, 2018

	OVERALL	
	High	Moderate
Risks	Inherent Risk	Residual Risk
Decreasing		
1. Risk of unauthorized access to confidential information from unauthorized and unmanaged devices	High	Low
17. Risk that employees are not aware of cyber security threats	High	Low
19. Risk of data loss or currpution by undeteced intruders	High	Low
20. Risk of data loss due to an undetected security control gaps	High	Moderate
4. Risk of unauthorized access to confidential information from unidentified threats and vulnerabilities	High	Low
5. Risk of unauthorized access to confidential information from unauthorized and unmanaged administrative privileges	High	Low
6. Risk that security audit logs are not used in cybersecurity management	Elevated	Low
Increasing		
10. Risk of unavailable information due to Ransomware (or other malware) and inadequate recovery mechanisms.	High	Moderate
13. Risk of unauthorized access to confidential information and exfiltration of the data from insiders	High	Moderate
Stable		
11. Risk of unauthorized access to confidential information from unauthorized network device changes	High	Elevated
12. Risk of unauthorized access to confidential information from external attackers	High	Moderate
14. Risk of unauthorized access to confidential information from a network breach	High	Elevated
15. Risk of unauthorized access to confidential information from wireless devices	High	Moderate
16. Risk of unauthorized access to confidential information from inactive system and application accounts	High	Moderate
18. Risk that in-house developed software has cyber security control gaps	High	Elevated
2. Risk of unauthorized access to confidential information from unauthorized and unmanaged software	High	Elevated
3. Risk of unauthorized access to confidential information from unmanaged hardware and software configurations	High	Moderate
7. Risk of unauthorized access to confidential information from email and web browsers	High	Moderate
8. Risk of unauthorized access to confidential information from malware	High	Moderate
9. Risk of unauthorized access to confidential information from network ports	Elevated	Moderate

Bank of Ozark – Control Assessment

Each sub-control receives a scored Control Rating. The total scoring equals the overall Control Effectiveness (Assurance Rating).

Inherent Risk + Control Effectiveness = Residual Risk



	CONTROLS and OVERALL ASSURANCE								RESIDUAL RISK	
CSC Std Control Objective	BOTO Control Name	BOTO Control Description	Owner	Frequency	Type	Method	Control Rating	Assurance Rating	Residual Risk	Comment
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	CSC 1.1 Active and Passive Device Discovery System	Management directed practice barcodes are affixed to new devices at procurement and once added to the network are scanned, inventoried and recorded in Ticketing System.	Dave Shackleford	Ongoing	Preventive	Hybrid	Strong	Strong	Low	Develop Asset Management Standard, and subsequent Procedures.

Benefits To Your Organization

1. The Risk framework is the foundation of your enterprise security strategy.
2. The Risk Dashboard is the core of your security reporting and presentations to the CEOs and Board.
3. Through Interactive dashboards, risks are more tangible for departments.
4. Security becomes a “center of excellence” for risk management.

Key Takeaways

1. Risk should be the cornerstone for your security program.
2. You need business buy-in.
3. How you think about risk is specific to your organization.
4. Keep things simple and interactive.
5. You need frameworks and visualization tooling.

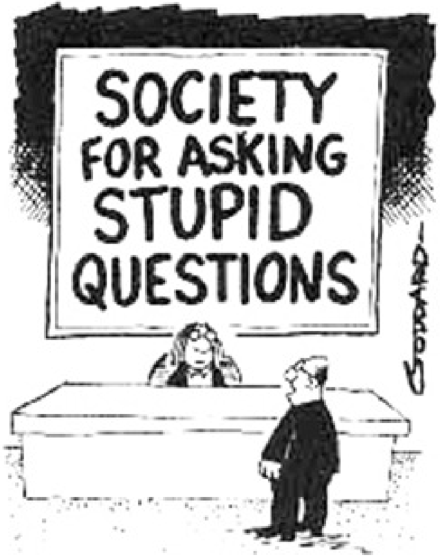
Apply What You Have Learned Today

- Next week you should:
  - Identify team members to form a security risk working group
  - Identify key stakeholders within the different business units/departments
- In the first three months following this presentation you should:
  - Have a BnL listing of all relevant risk scenarios based on initial meetings and feedback from the business
  - Adopt and customize a tailored control framework, at the control objective level
- Within six months you should:
  - Have an initial understanding of your key risks by department, and resulting critical controls
  - Plan to incorporate control audit scores into the risk picture
  - Have an low confidence security strategy/control mitigation plan based on the risks the business has told you are most critical to mitigate

Questions

Rick Patterson

rpatterson123@gmail.com



"Excuse me, but is this The Society for Asking Stupid Questions?"