

CYBERSECURITY & TECHNOLOGY RISK: AN ERM PERSPECTIVE

**NYSICA 6th Annual Fraud, Integrity, and
Controls Conference**

Destination Check

- An increasingly competitive global marketplace has organizations (whether publicly traded, private companies, government agencies, and non-for-profits) clamoring for better information assurance and the additional business development facilitation and performance insight enabled by technology. While IT professionals have the technical expertise necessary to ensure the secure configuration of IT hardware or proper deployment of technology solutions, their solutions frequently lack the internal control professional's perspective and ability to understand the complicated business implications, governance challenges, and risks associated with technology.
- This session will help attendees look and consider cybersecurity and technology risks from both the Board – especially Audit Committee and the enterprise risk professional's perspective (whether internal control, auditor or financial perspective). Governmental agencies and industry rely on IT assets such as computers, networks, and data to interact and deliver value to the end-user (e.g., constituent or customer). Protecting these assets, as well as the constituent/customer relationship, requires that organizations of all sizes understand, assess, remediate and repair unmitigated threats to remain relevant in the marketplace and to take advantage of emerging business or service delivery opportunities.

TODAY'S "FLIGHT PLAN" – KNOWLEDGE TRANSFER



Joel Lantz


*CPA.CGMA.CITP.CFF, CISA,
CISM, CISSP, CFE*

Joel is a member of the Business Environment & Concepts (BEC) Subcommittee (of the CPA Exam Content Committee) and the immediate past Chairman of the AICPA's Information Management and Technology Assurance Executive Committee.

Joel also serves as a reference (non-voting) member of a \$1.2 Billion non-profit's audit committee.

Prior to starting his niche IT Audit, Information Security and Risk Management practice in 2001, Joel was a Technology Risk Partner in Arthur Andersen's Business Risk Consulting and Assurance Practice, a Manager at Price Waterhouse and a Vice President and Audit Manager The Chase Manhattan Bank.

Joel received both his BBA (Accounting) and MBA (Information Systems) from Pace University.

Technology Risk Advisory Practice	Thought Leadership	Graduate School Professor
<p>Joel's niche CPA practice provides technology governance, IT Audit, Information Security Management, Cyber Risk Assessment and IT Vendor Oversight services sectors since 2001.</p> 	<ul style="list-style-type: none">• Editorial Board member of "The CPA Journal."• Previously chaired both the NYSSCPA Technology Assurance and Information Technology Committees.• Immediate Past Chair of the AICPA's Information Management and technology Assurance Executive Committee and previously Chaired the AICPA's CITP Specialist Credential committee.• Co-chaired the AICPA's 2010 & 2011 Top Tech Task Force.• IIA – Long Island Chapter Board of Governors.	<p>Visiting Assistant Professor in the School of Business at The State University of New York – College at Old Westbury. Courses instructed include;</p> <ul style="list-style-type: none">• Auditing,• Advanced Assurance• Forensic Accounting• Accounting Information Systems• Accounting Research. <p>Adjunct Associate Professor at NYU Stern Graduate School of Business teaching courses in the M.S. in Accounting program. Courses taught include:</p> <ul style="list-style-type: none">• IT Auditing• Internal Controls & Accounting Information Systems. <p>Seminar and CPE Presenter for AICPA, NYSSCPA, IIA, and private CPE providers.</p> <p>Publications include Journal of Accountancy, The CPA Journal and The Risk Management Association Journal.</p>



Disclaimers

- I am my own person and do not speak for, endorse, represent, etc., any of the organizations, associations or universities that I am affiliated with. In other words, my opinions are my own and represent what I personally believe.
- I am not endorsing any company, service, product nor are any endorsements implied.
- I am presenting today in “the spirit of professional knowledge sharing and transfer.”

You (not a
consultant or a
presenter) are the
“Pilot” of your
plane and are
ALWAYS
accountable



Some Fundamentals Before We Start Our Journey



Photo by [Alexis Huot](#) on [Unsplash](#)

Lessons I Learned from Sitting on an Audit Committee



Cybersecurity is important – but it is not the only technology-related issue that we **MUST** discuss.



Technology is important – but it is not the only risk that we **MUST** discuss.



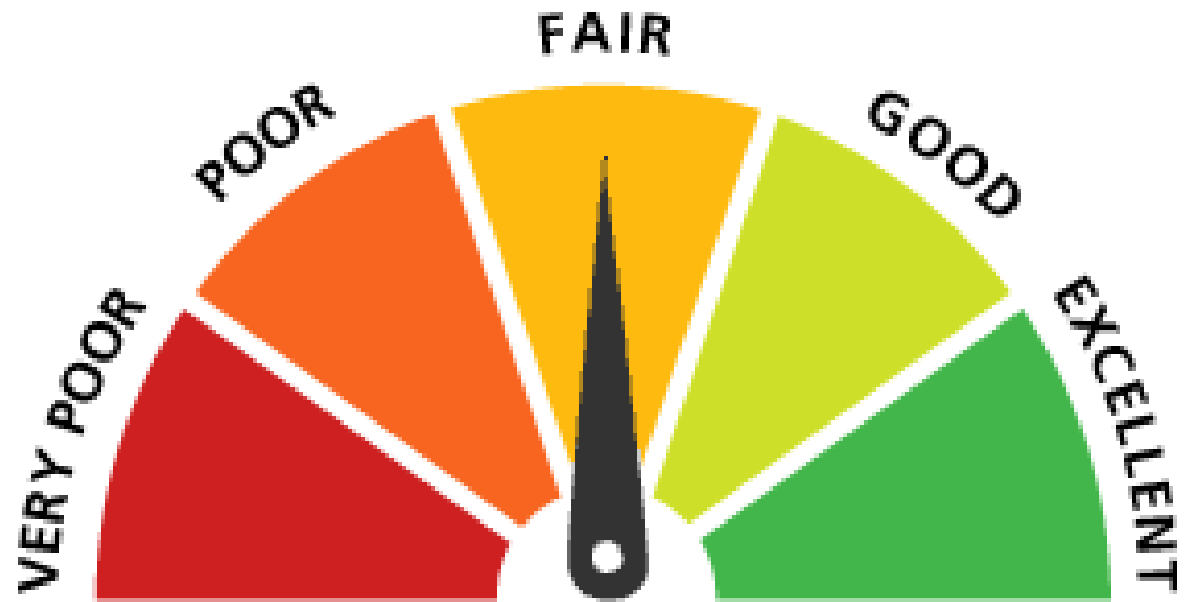
Risk is important – but is not the only governance issue that we **MUST** discuss.



Oh, and by the way, we **MUST** oversee the internal audit function, external public accountant, “coordinate” with any risk management initiatives - review policies, financial reports, complaints, fraud allegations, and perform any additional tasks assigned by the Chair of the Board.

Other things are important too
Overcoming the realistic time crunch

The *NECESSITY*
of Effective
Communication



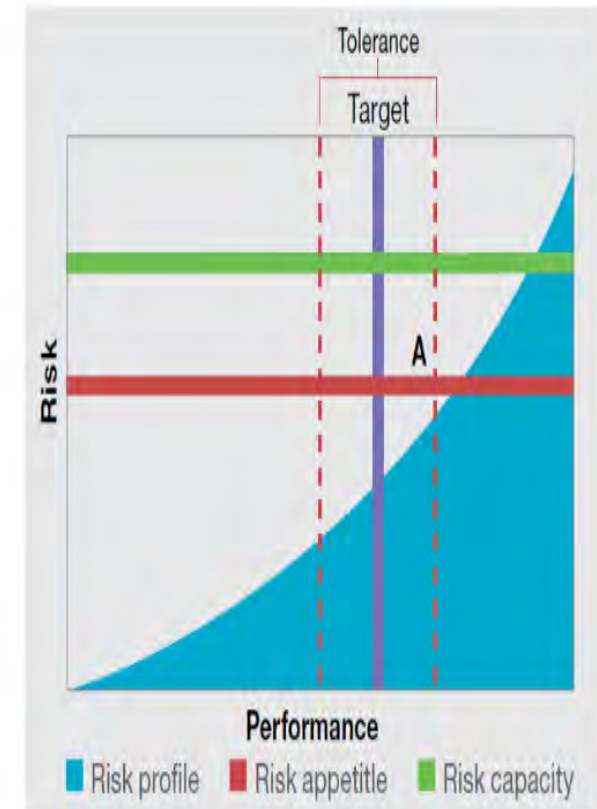
Risk Profile (From: COSO ERM)

- An organization manages risk to strategy and business objectives in relation to its risk appetite.
- Risk appetite:
 - The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
- Manages risk in the context of achieving strategy and business objectives – not as individual risks.

Introduces a new depiction referred to as a risk profile
Incorporates:

- Risk
- Performance
- Risk appetite
- Risk capacity

Offers a comprehensive view of risk and enables more risk-aware decision making



Classic and Evolving Technology Musts

- Alignment of technology with business objectives
 - “Fiduciary” use of technology-related investments
 - Facilitating/Enabling the mission
 - Safeguarding Assets (Data and Information Processing)
 - Compliance with regulatory and legal expectations
-
- Social Media (Protect reputation and customer engagement)
 - Strategic use and reliance on service providers (including cloud computing solutions)
 - Mobile and other IoT strategies
 - Data Governance (including Big Data, Data Analytics and Continuous Monitoring)
 - Privacy
 - Implementation and Monitoring of Business Systems
 - Impact of Technology Risk on Reputation

Yet Cybersecurity is the Golden Child of MUST



Some may believe that concerns over cybersecurity are exaggerated and as in the past, cost-effective threats can be easily managed – and that management of the problem can be relegated as in the past to the IT Department.



Others, including professional associations, reputable consultancies, think tanks, and the media, believe that this time it is different.

Cybersecurity is a significant business issue that dramatically impacts the organization's relationship with its customers, profitability and reputation.

Because technology is so embedded into the business – from sourcing customers to receiving and making payment – and to maintaining financial records that no longer have paper support, managing cybersecurity risks can no longer be delegated to someone other than the person or group primarily responsible for the business.



Many Board members and Executives have come to the conclusion that it is a Business issue – (**TARGET AND SONY ATTACKS WERE THE TURNING POINT!!** (or any other attack that has received significant media coverage).



In many aspects the theoretical differences between information security and cyber security are immaterial as far as Audit Committee and Executive Management responsibilities go.

So Why Does
Cybersecurity
Keep Some
Audit
Committee
Members Up
At Night?

**Assumption
that breach
will occur –
AND
surviving the
aftermath of
“the event”**

- Amount of potential loss (financial, reputational, lost opportunities)
- Sophistication and purpose of the attack
- Frequency and velocity of the attacks
- Information outside the organization
- Negative publicity
- Evolving insurance coverage and underwriting requirements
- Lawsuits from stakeholders (shareholders, customers, partners, unforeseen parties)
- Regulatory expectations and “suggestions”
- “Helpful advice” from accounting, law firms and vendors
- Guidance from recognized authorities and associations.



Guidance Issued By The NACD

The National Association of Corporate Directors (NACD), issued a publication, "Cyber-Risk Oversight Handbook." The handbook identified five principles that Board Members should consider in governing Cybersecurity.

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

The background of the slide features several sets of thin, curved lines in light gray and blue, creating a sense of motion and depth. These lines are primarily located on the left and right sides of the slide, framing the central content.

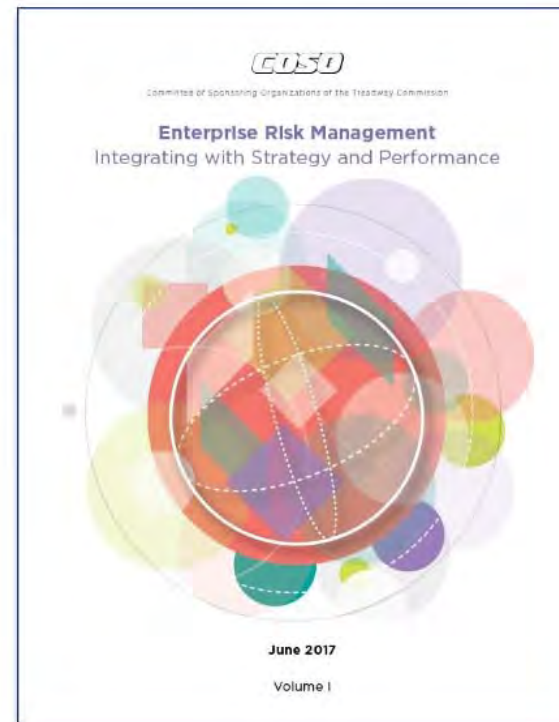
.....and Don't Forget the Firms and "Other Experts"

- Many of the firms have developed and distributed to the audit committee recommended questions that committee members should be asking of management.
- These questionnaires can be used to effectively jumpstart discussions between the audit committee and management on the more critical governance issues.
 - Sometimes a neutral document that helps balance governance vs. risk
 - May refer to more detailed frameworks
- Sometimes not so neutral and provides biased suggestions.

Quick Talk about Enterprise Risk Management



Enterprise Risk Management Framework: Integrating with Strategy and Performance



Enterprise Risk Management



- The culture, capabilities and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in **creating, preserving and realizing value**.
- Every entity exists to **provide value to its stakeholders**.
- All entities **face risk** in the pursuit of value.
- Risk affects an organization's ability to achieve its strategy and business objectives,
- Management determines the amount of risk the organization is prepared and willing to accept.
- **Effective ERM helps boards and management to optimize outcomes with the goal of enhancing capabilities to create, preserve, and ultimately realize value.**

The Updated Framework Focuses on Integration While Emphasizing and Creating Value



- Integrating ERM with business practices results in better information that supports improved decision making and leads to enhanced performance helping organizations to:
 - Anticipating risks earlier or more explicitly, opening up **more options for managing the risks**
 - Identifying and **pursue existing and new opportunities**
 - **Responding to deviations** in performance more quickly and consistently
 - Developing and reporting a more comprehensive and consistent **portfolio view of risk**
 - Improving collaboration, trust, and information sharing
- **Links value to risk appetite and the ability to manage risk to acceptable levels**

20 key principles within each of the five components



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals



Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives



Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View



Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management



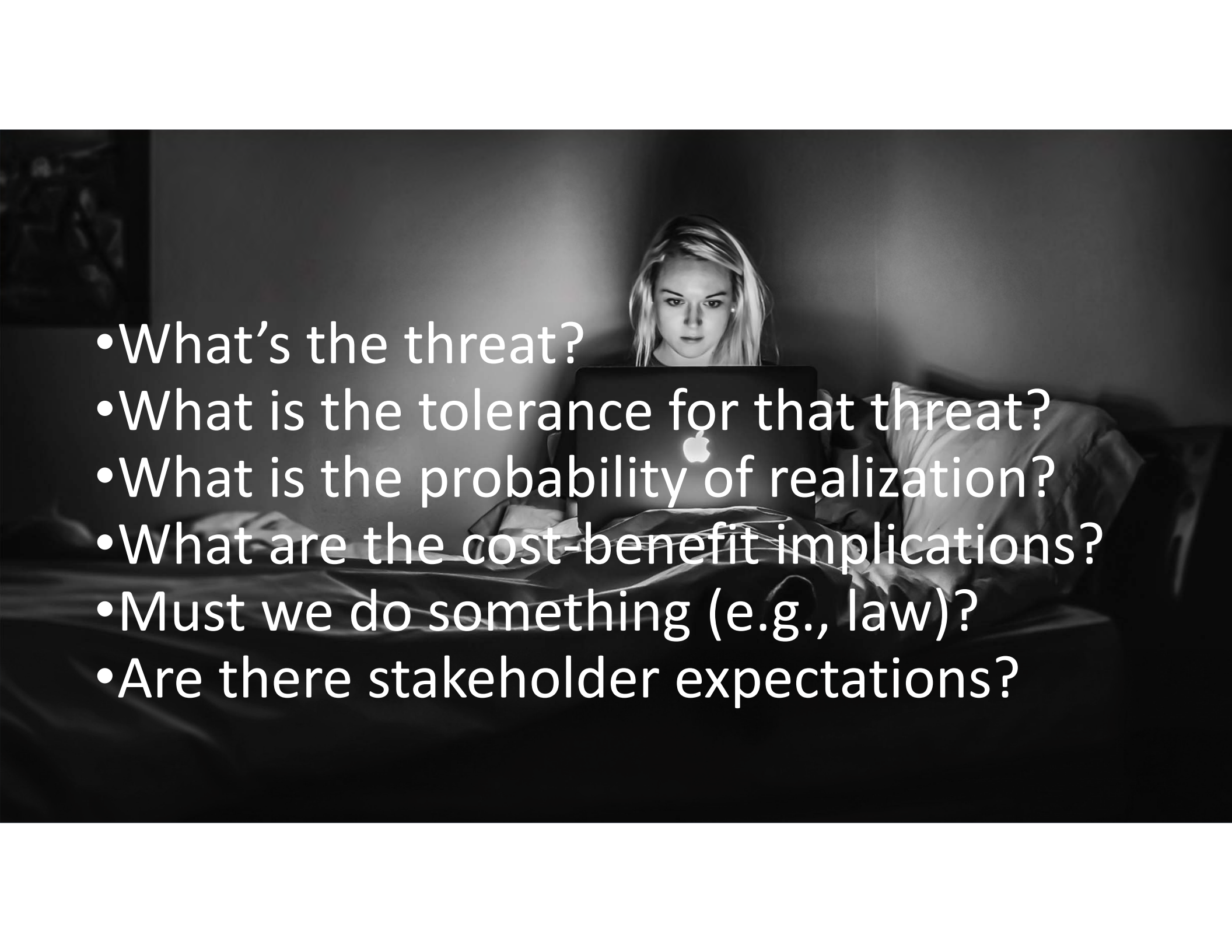
Information, Communication, & Reporting


18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Enough with this
ERM stuff – are we
safe and protected
or not?

Photo by Aziz Acharki on Unsplash



- 
- What's the threat?
 - What is the tolerance for that threat?
 - What is the probability of realization?
 - What are the cost-benefit implications?
 - Must we do something (e.g., law)?
 - Are there stakeholder expectations?



I've met a lot of people in my career. One fear everyone from CEO to technology administrator share – no one wants to get hacked on their watch.



Photo by [Samuel Zeller](#) on [Unsplash](#)

You must know
the inventory
of the
technology
assets that you
are responsible
for to achieve
security goals

The 30 Second Controls Audit?

Auditor: Can you provide me with a copy of a “reasonably current” inventory of all technology assets (hardware, software, third-party relationships, etc.)?

Management: Can we have a week or two to gather?

Auditor: I’m just wondering that if you don’t have one available how are you:

- Managing business continuity issues?

- Know the priority and classification of assets to be protected?

- Know where critical resources are stored?

- Monitor what access vendors have to our assets?

- Can we account for everything we are paying for?

- How do we know which vulnerabilities need to be remediated?

- How do we know what needs to be logged and monitored?



...and speaking
of auditing –
leverage core
audit planning
process to
assess security



DETERMINE OBJECTIVE



RESEARCH AND
POTENTIAL THREAT/RISK
IDENTIFICATION



OBTAIN AN
UNDERSTANDING



DOCUMENT THE
UNDERSTANDING



CONFIRM THE
UNDERSTANDING
(WALKTHROUGH)



FINALIZE POTENTIAL
THREAT/RISK
IDENTIFICATION

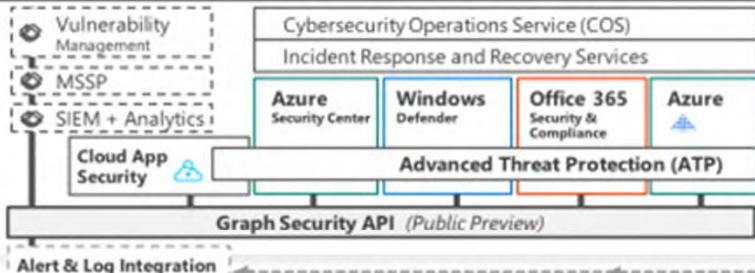


IDENTIFY CONTROLS AND
RISK MITIGANTS



DETERMINE RESIDUAL
RISKS AND FURTHER
ACTION

Security Operations Center (SOC)



Cybersecurity Reference Architecture

May 2018 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Information Protection

Conditional Access – Identity Perimeter Management

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

- Office 365
- Data Loss Protection
- Data Governance
- eDiscovery

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL

- Threat Detection
- SQL Encryption & Data Masking
- SQL Info Protection (Preview)

Azure SQL

- Threat Detection
- SQL Encryption & Data Masking
- SQL Info Protection (Preview)

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP

Endpoint DLP

- Endpoint DLP



Identity & Access

Azure Active Directory

Azure AD Identity Protection

- Leaked cred protection
- Behavioral Analytics

Azure AD PIM

- Multi-Factor Authentication

Azure AD B2B

- Azure AD B2C

Hello for Business

- MIM PAM

Azure ATP

- Azure ATP

Active Directory

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

ESAE Admin Forest

- ESAE Admin Forest

Clients

Unmanaged & Mobile Devices

- Intune MDM/MAM

Managed Clients

- System Center Configuration Manager

Windows Defender ATP

- Secure Score
- Threat Analytics

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction

App control

- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

S Mode

- S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

- Extranet
- Intranet Servers

3rd party IaaS

- Security Appliances

Microsoft Azure

- Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Windows Server 2016 Security

- Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs

- Azure Stack

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs)

- Privileged Access Workstations (PAWs)

IoT and Operational Technology

Windows 10 IoT

- Windows 10 IoT

Azure IoT Security

- Azure IoT Security

Azure Sphere

- Azure Sphere

IoT Security Maturity Model

- IoT Security Maturity Model

IoT Security Architecture

- IoT Security Architecture

Azure Sphere

- Azure Sphere

IoT Security Maturity Model

- IoT Security Maturity Model

IoT Security Architecture

- IoT Security Architecture

IoT Security Architecture

- IoT Security Architecture

IoT Security Architecture

- IoT Security Architecture

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Security Development Lifecycle (SDL)

- Security Development Lifecycle (SDL)

Compliance Manager

- Compliance Manager

Compliance Manager

- Compliance Manager

Compliance Manager

- Compliance Manager

Compliance Manager

- Compliance Manager

Compliance Manager

- Compliance Manager

Compliance Manager

- Compliance Manager

Trust Center

- Trust Center

Trust Center

- Trust Center

Trust Center

- Trust Center

Trust Center

- Trust Center

Intelligent Security Graph

- Intelligent Security Graph

Intelligent Security Graph

- Intelligent Security Graph

Intelligent Security Graph

- Intelligent Security Graph

Intelligent Security Graph

- Intelligent Security Graph



AWS Shared Responsibility Model

CUSTOMER

RESPONSIBILITY FOR
SECURITY 'IN' THE CLOUD

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA
ENCRYPTION & DATA INTEGRITY
AUTHENTICATION

SERVER-SIDE ENCRYPTION
(FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC
PROTECTION (ENCRYPTION,
INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR
SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

TECHNOLOGY CHECKLIST



Businesses are quickly deploying all kinds of technology. Different kinds of technologies come with different risks and strategies to protect them. This checklist is designed to help you identify the technology in your business you need to protect. In addition, there are some basic security tips, considerations and links to resources that can help you learn more to detect, respond to and recover from cyber incidents.

<input type="checkbox"/> WIFI	<input type="checkbox"/> FILE SHARING	<input type="checkbox"/> USB
<input type="checkbox"/> ROUTERS	<input type="checkbox"/> COPIERS/PRINTERS/FAX MACHINES	<input type="checkbox"/> WEBSITE
<input type="checkbox"/> FIREWALLS	<input type="checkbox"/> CLOUD SOLUTIONS	<input type="checkbox"/> SOCIAL NETWORKING
<input type="checkbox"/> MOBILE DEVICES	<input type="checkbox"/> VPN	<input type="checkbox"/> POINT OF SALE
<input type="checkbox"/> EMAIL	<input type="checkbox"/> SWITCHES	<input type="checkbox"/> 3RD PARTY VENDORS

WIFI:

- Use strong administrative and network access passwords
- Use strong encryption (WPA2 and AES encryption)
- Use separate WiFi for guests
- Physically secure WiFi equipment
- Get savvy about WiFi hotspots - Limit accessing sensitive information on public WiFi - Use VPN when using public WiFi

VIRTUAL PRIVATE NETWORK (VPN):

- Use strong passwords, authentication and encryption
- Limit access to those with valid business need
- Provide strong antivirus protection to users

NETWORK DEVICES:

Routers and Switches

- Use a network monitoring app to scan for unwanted users
- Restrict remote administrative management
- Log out after configuring
- Keep firmware updated
- Use strong passwords

Firewalls

- Default rules should block everything that is not specifically necessary for the business

USBs:

- Scan USBs and other external devices for viruses and malware when connected
- Only pre-approved USBs allowed in company devices
- Educate users about USB risks



STOP | THINK | CONNECT

WEBSITE:

- Keep software up to date
- Require users to create strong passwords to access
- Prevent direct access to upload files to site
- Use scan tools to test your site's security - many are free
- Register sites with similar spelling to yours
- Run most current versions of content management systems or require web administrator/hosts to do the same

MOBILE DEVICES:

- Keep a clean machine: Update security software on all devices
- Delete unneeded apps
- Secure devices with passcodes or other strong authentication such as a finger swipe and keep physically safe
- Encrypt sensitive data on all devices
- Make sure "find device" and "remote wipe" are activated

EMAIL:

- When in doubt, throw it out: Educate employees about remaining alert to suspicious email
- Provide all email recipients with an option to opt off your distribution list
- Require long, strong and unique passwords on work accounts
- Get two steps ahead: Turn on two-factor authentication



FILE SHARING:

- Restrict the locations to which work files containing sensitive information can be saved or copied
- If possible, use application-level encryption to protect the information in your files
- Use file-naming conventions that are less likely to disclose the types of information a file contains
- Monitor networks for sensitive information, either directly or by using a third-party service provider
- Free services do not provide the legal protection appropriate for business

POINT OF SALE (POS):

- Make unique, strong and long passwords and change regularly
- Separate user and administrative accounts
- Keep a clean machine: Update hardware and software as needed
- Avoid web browsing on POS terminals
- Use antivirus protection

OTHER:

Secure Disposal

- Be aware that many devices, not just PCs and phones, have memory. Know how to clean old data before disposing

Internet of Things (IoT)

- Consumer Protection and Defense Recommendations
- Isolate IoT devices on their own protected networks and change default passwords
- Know what information is being collected and how and where it's being stored and protected
- Consider whether IoT devices are ideal for their intended purpose
- Purchase IoT devices from manufacturers with a track record of providing secure devices
- When available, update IoT devices with security patches (Source: www.ic3.gov)

SOCIAL NETWORKING:

- Create page manager policies and roles
- Limit administrative access
- Require two-factor authentication
- Secure mobile devices

CLOUD AND OTHER 3RD PARTY VENDORS:

- Discuss the approach to security and codify in any agreements and contracts

COPIERS/PRINTERS/FAX MACHINES:

- Understand that digital copiers/printers/fax machines are computers
- Ensure devices have encryption and overwriting
- Take advantage of all the security features offered
- Secure/wipe the hard drive before disposing of an old device
- Disable the web management interface or change the default password

Consumer Reports - Privacy Tips for the Internet of Things

<http://www.ic3.gov/media/2015/150910.aspx>

FTC - Careful Connections: Building Security in the Internet of Things

<http://1.usa.gov/1Vettp>



STOP | THINK | CONNECT

“Plain Talk” on Frameworks and Why “We” Like Them

Recognized Frameworks

- SOC for Cybersecurity
- SOC for Service Providers
- NIST Cybersecurity Framework
- NIST Special Publications
- CoBIT
- CERT (OCTAVE, Insider Threats)
- ISO
- Regulatory (FFIEC, HIPAA, State Laws)
- PCI
- Center for Internet Security
- OWASP (Web Applications)

Why We Like Them

- Unbiased
- Peer Reviewed
- Relatively Low Cost
- Common Language
- Recognized as Best or Good Practices
- Baselines for Stakeholders can Assess Against (e.g., customers)
- “Standard of Reasonableness?”
- Don’t have to recreate

[Services](#)[News](#)[Government](#)[Local](#)[Location](#)[Translate](#)

Office of Information Technology Services

[Services](#)[Get Help](#)[Cyber Security](#)[Policies](#)[Procurement](#)[Media Center](#)[About ITS](#)[Employees](#)

ITS Policies

[HOME](#) » [POLICIES](#)

Statewide technology policies and guidelines set standards and define best practices for the State's IT community. All statewide technology policies are available by category and can be ordered by number, date published, and date modified date. A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "[NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary](#)".

More information about the process for establishing NYS policies is available in the [Process for Establishing Enterprise Information Technology Policies, Standards, and Guidelines \(NYS-P09-003\)](#).

Center for Internet Security (CIS)
Critical Security Controls (cisecurity.org)

Basic CIS Controls

- | | | | |
|---|---|---|---|
| 1 | Inventory and Control of Hardware Assets | 4 | Controlled Use of Administrative Privileges |
| 2 | Inventory and Control of Software Assets | 5 | Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers |
| 3 | Continuous Vulnerability Assessment and Remediation | 6 | Maintenance, Monitoring and Analysis of Audit Logs |

Foundational CIS Controls

- | | | | |
|----|--|----|---|
| 7 | Email and Web Browser Protections | 12 | Boundary Defense |
| 8 | Malware Defenses | 13 | Data Protection |
| 9 | Limitation and Control of Network Ports, Protocols, and Services | 14 | Controlled Access Based on the Need to Know |
| 10 | Data Recovery Capabilities | 15 | Wireless Access Control |
| 11 | Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches | 16 | Account Monitoring and Control |

Organizational CIS Controls

- | | | | |
|----|---|----|--|
| 17 | Implement a Security Awareness and Training Program | 19 | Incident Response and Management |
| 18 | Application Software Security | 20 | Penetration Tests and Red Team Exercises |

Converting Critical Security Controls Into Business Oversight Considerations (Top 5 Only)

Too often we hear why these controls can't be implemented – especially from IT Operations.....

CSC 1 Inventory of Devices	CSC 2 Inventory of Software	CSC 3 Vulnerabilities	CSC 4 Admin Privileges	CSC 5 Secure Configurations
<ul style="list-style-type: none">• How much is our IT budget?• Do we reconcile inventory to accounting records?• Have we assigned custodial responsibilities?	<ul style="list-style-type: none">• Do we have the “right mix” of licenses?• Can we get sued?• Do we know what is running on our systems?	<ul style="list-style-type: none">• What’s acceptable and what is not?• Are the vulnerabilities indicative of other problems?• Are things good enough that we can pass a “real” pen test?	<ul style="list-style-type: none">• Do we limit access on a need-to-have basis?• Are we enforcing segregation of responsibilities?• Do we have the audit trails to hold privileged employees accountable for their actions?	<ul style="list-style-type: none">• How do we determine what we configure?• Does someone review what gets configured?• How do we compare against outside practices (e.g., good practices)?

*.....Yet, these are fundamental business management controls –
The types of questions Audit Committees can and should be asking about.*

What's In Your Audit Committee Deliverable?

“Look Mom, no technical words!!!!!!”

CSC1 Inventory of Devices	CSC2 Inventory of Software	CSC4 Vulnerabilities	CSC5 Admin Privileges	CSC3 Secure Configurations
<ul style="list-style-type: none">•Need software to monitor changes.•Change control process needs to be enhanced.	<ul style="list-style-type: none">•Need tracking tool to monitor for software licenses.•Need to reconcile payments to vendors to existing software.•Need to enhance controls over desktop software and related risks.	<ul style="list-style-type: none">•Vulnerability remediation practices significantly violates established policies.•Only 40% of eligible assets are scanned.•Vulnerability remediation KPI is 35% below standard.	<ul style="list-style-type: none">•All practices comply with current expectations and policies.	<ul style="list-style-type: none">•Configuration strategies need to be developed and standardized.•Automated tool to monitor compliance with policy needed.•Exception process needs to be defined.CSC3 <p>Secure Configurations</p> <ul style="list-style-type: none">•Configuration strategies need to be developed and standardized.•Automated tool to monitor compliance with policy needed.•Exception process needs to be defined.

Key Issues: Does Management understand the gaps and is action being taken?

Does the information presented by Management match Internal Audit's cumulative understanding?

Red-Yellow-Green Dashboards (Heat maps)

CoBIT 4.1 Maturity Level Emphasis

(NOTE: Current Version is 5)

CoBIT DOMAINS	SECTION	TARGET MATURITY	ASSESSED MATURITY	RESIDUAL RISK LEVEL	PROBABILITY	IMPACT	REMEDATION PRIORITY
PO1 Define a Strategic IT Plan	IT Mgt.	Managed(4)	Managed(4)	Low	Low	Low	n/a
PO2 Define the Information Architecture	IT Mgt.	Repeatable(2)	Repeatable(2)	Low	Medium	Medium	Medium
PO3 Determine Technological Direction	IT Mgt.	Defined(3)	Defined(3)	Low	Medium	Medium	Medium
PO4 Define the IT Processes, Organisation and Relationships	IT Mgt.	Defined(3)	Defined(3)	Low	Low	Medium	Low
PO5 Manage the IT Investment	IT Mgt.	Defined(3)	Defined(3)	Low	Low	Low	n/a
PO6 Communicate Management Aims and Direction	Risk Mgt.	Defined(3)	Defined(3)	Low	Low	Low	n/a
PO7 Manage IT Human Resources	IT Mgt.	Defined(3)	Defined(3)	Low	Low	Low	n/a
PO8 Manage Quality	IT Mgt.	Defined(3)	Defined(3)	Low	Low	Medium	Low
PO9 Assess and Manage IT Risks	Risk Mgt.	Managed(4)	Managed(4)	Low	Medium	Medium	Medium
PO10 Manage Projects	IT Mgt.	Defined(3)	Defined(3)	Low	Low	Low	n/a
AI1 Identify Automated Solutions	Business Solutions	Defined(3)	Defined(3)	Low	Low	Low	n/a
AI2 Acquire and Maintain Application Software	Business Solutions	Defined(3)	Defined(3)	Low	Low	Medium	Low
AI3 Acquire and Maintain Technology Infrastructure	Business Solutions	Defined(3)	Defined(3)	Low	Low	Low	n/a
AI4 Enable Operation and Use	Business Solutions	Defined(3)	Defined(3)	Low	Low	Low	n/a
AI5 Procure IT Resources	Business Solutions	Defined(3)	Defined(3)	Low	Low	Low	n/a

FFIEC (Banking) IT Audit Dashboard

Handbook/Focus	Previous IT Audit Assessment	Current Monitoring Results	Pattern	Next Scheduled IT AUDIT
Business Continuity				'16-Move up 6 mos.
Development & Acquisition				'17- Hold
Internal Information Security				'17-Move up 3 mos.
Cybersecurity				'16-Multiple Project
Management				'16-New Guidance
Operations				'18-Hold
Outsourcing				'17-Hold



Vulnerability Assessment & Pen Testing

- Too much “Scan and Dump” and not enough insightful analysis.
- What does all the information mean and what are we supposed to do with it?
- What exactly is a “Pen Test” and what do the results really mean?
- Who and how is following up on this and why are we waiting until next year to see if remediated?
- Why are we spending money on Pen Testing when we don’t have a working vulnerability remediation program (and automated tool)?



Patch and Vulnerability Management- The “Diet and Exercise” of Cybersecurity

Convert the Most Technical Issues Into Something a Business Person Can Understand & Act Upon

Top 10 Vulnerability Exposure

	%/# Assets Impacted	%/# High Assets Impacted	Exploit Available?	Fix By Date
#1	100/100	25/25	Yes	30 days
#2	50/50	20/20	Yes	45 days
#3	25/25	15/15	Yes	75 days
#4	20/20	10/10	No	TBD
#5	10/10	90/90	No	TBD

Vulnerability Remediation Days Outstanding

Risk Level	0-30 Days	30-60 Days	60-90 Days	90-120 Days	Over 120
5	15	12	8	2	1
4	25	20	13	6	2
3	45	38	24	12	5
2	120	110	90	70	35
1	500	450	375	300	275

“We found that ten vulnerabilities accounted for almost 97% of the exploits in 2014. The remaining 3% consists of 7,000,000 other vulnerabilities. Most attacks exploited known vulnerabilities where a patch has been available for months, often years. Of the vulnerabilities detected in 2014 we found more dating back to 2007 than from any year since.” –VERIZON BREACH REPORT 2015 EXEC. SUMMARY

Illustrative “Bum of the Month” Map (Who is responsible for the RED Boxes?)

	MKT	CIO	CISO	User	Vendor	Audit
Web	X			X	X	?
Routers		X	X			?
Firewalls		X	X			?
Servers		X	X		X	?
Desktop	X	X		X	X	?
Core Application		X	X	X	X	?
Cloud	X		X	X	X	?
Mobile		X	X	X	X	?
Testing			X			X



Other Technology Risks

Data Governance

Outside of cybersecurity, perhaps no other enterprise-related IT risk management topic has captured executive management and board attention like data governance.

From an enterprise perspective, which users or departments own the company's data, what they can do with it, and how they should protect it have always been topics of discussion and, in some cases, sources of conflicts.

The recent scandal at Facebook involving data acquired by the company and sold to third parties has increased attention paid to this concern.



Why is Data Governance a Challenge?

- The problem facing most companies is that while data is an asset, most of them do not treat it as such.
 - Business digitilation
 - CRM reliance and strategies
 - Rise of data analysis and business intelligence

Vendor Management & Cloud Computing

- Cloud computing has grown so popular and useful that technology companies to whom agencies outsource their systems (i.e., cloud service providers) now use cloud providers such as Amazon Web Services (AWS) and Microsoft Azure themselves to deliver services cost effectively and minimize the potential of loss from the most pervasive threats.
- Such vendors will often advertise and promote the reputation of AWS and Azure in selling their services; often, if the agency does due diligence or vendor management over its vendor, it relies on the vendor's representation that using AWS and Azure provides "best-in-class" security to the customer.
- Both AWS and Azure communicate that security is a joint responsibility between the organizations and the technology service provider, and that, as part of its vendor management oversight, the endpoint customer should determine and confirm that its technology service provider is addressing those responsibilities.



End Users – How to Manage? (or Make it Happen!!!)

- In some respects, organizations have traditionally held users accountable for their use of technology, although frequently this was in name only.
- In other organizations, management expects the central IT department to provide significant support and, in many cases, “hand-hold” business owners to meet their needs and mitigate any circumvention of controls not compensated for by pervasive IT department practices and expertise.

Critical risk considerations for these tools center around traditional development and application controls.

Can the company rely on the controls used in the tool's development process, and is the analysis and resultant calculation reliable?

Are the data sources used for the analysis accurate and timely?

Do processing and analysis consider all the data processed and exclusions?

From an ERM perspective, a consistent strategy needs to be adopted. As with end-user computing, educating and communicating common expectations are critical for areas that involve the accuracy and reliability of results, such as user acceptance and stress testing.

Artificial Intelligence and Automation

The Cost of Risk Management

- The cost of seizing new business opportunities and entering new markets is an increase in a company's risk profile.
- While most agree on the necessity of managing this increased risk, there is general disagreement on the quantity of risk management needed and which risk mitigation activities provide minimal value to the enterprise, including those procedures that are duplicative.
- Most business executives, however, understand the need for these controls.
- The recent focus on extensive documentation requirements also raises significant concerns related to the cost and added value of risk management provided.



Conclusion – Meeting The Challenge



The ability to manage technology risk is a critical component of any organization's ERM effort.



COSO's new *Enterprise Risk Management–Integrated Framework* provides companies with the flexibility and tools needed to align technology risk with strategic goals and business objectives.



Cybersecurity threats and computer errors will always be factors that hinder an organization's success, reputation, and value.



The new ERM framework provides a process for companies to make appropriate investments for the given risk appetite and tolerances, helping to ensure that risk-adjusted returns provide necessary funding for the long-term well-being of the enterprise.

FOR FURTHER
INFORMATION

*Thank you for attending
today's conference.*

*Should you have any follow-
up questions please do not
hesitate to call or email me.*

*Don't forget to visit my
website for articles,
columns and my blog.*

- Contact Joel directly at:

Joel Lanz

Joel Lanz, CPA, P.C.

471 N. Broadway

Jericho, NY 11753

(516) 933-3662

jlanz@joellanzcpa.com

www.joellanzcpa.com

<http://www.linkedin.com/in/joellanz>