Homework:

- Send Alex a private message asking what section of HiTrust to look at
  - *1 page response about a HiTrust Objective*
  - *Submit PDF to homework engine*
  - *HiTrust PDF on homework engine +*

- Submit your **UPDATED** resume to be reviewed by SecDev by Sunday 11:59pm (October 28, 2018)

RISK MANAGEMENT

BY ALEXANDER BITAR

Who I Am

- **B.S. Business Administration – Spring 2017**
  - *Concentration: MIS*
  - *IS & T Auditor Internship – Sodexo – 2017*

- **Master of Science in MIS – Spring 2019**
  - *Security Development Track*
  - *Certificate in Information Assurance*
  - *TA for MGS 351*
  - *Information Risk Assurance Internship - Blue Cross Blue Shield of WNY – 2018*
  - *President of ISACA Student Group UB*

What is **risk?**

Is Skydiving risky?

Skydiving Statistics

Year	Skydiving Fatalities in U.S.	Estimated Annual Jumps	Fatalities Per 1,000 Jumps
2017	24	3.2 million	0.0075
2016	21	3.2 million	0.0065
2015	21	3.5 million	0.0061
2014	24	3.2 million	0.0075

Agenda

- What is risk?
- What do we do with Risks?
  - *Personally*
  - *An organization*

Risk

- The **potential** of **losing** something of **value.**

- **Information security risks** – are risks as they apply to data assets.

Risk Management

- Information Security Policies
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Encryption
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance
- Career and Workforce Development
- Security Awareness

Risks are not only external or technical..

- Financial
- Vendor Driven
- Accidental
- Internal
- Civil
- Legal
- Natural Disasters or Environmental

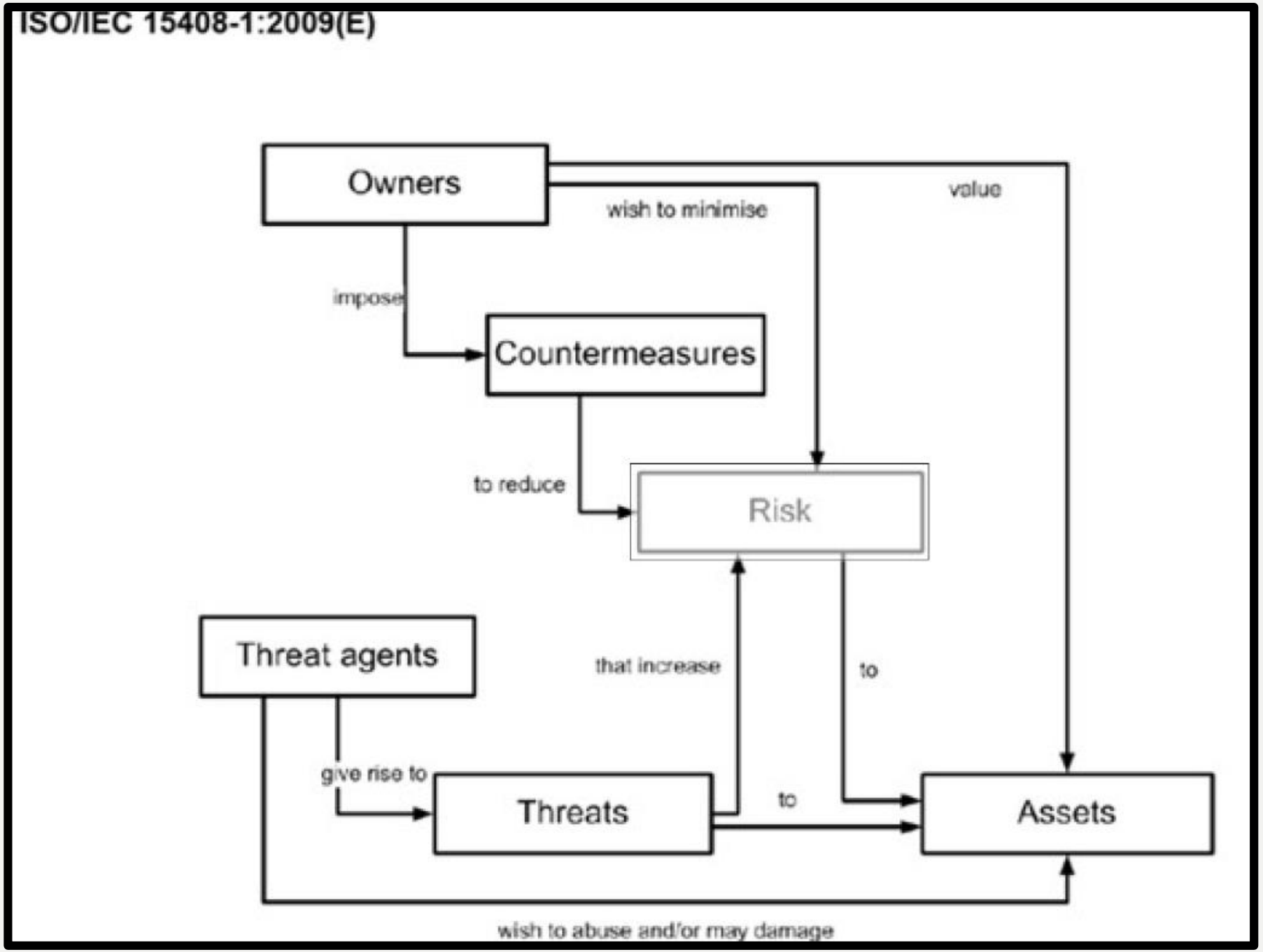
Impact x Likelihood

- **Impact** - If a threat were to materialize, how could it affect our business?
- **Likelihood** –what is the probability of a threat materializing?

- **Risk** = **Likelihood** X **Impact**
  - Likelihood - **chance** of a risk event occurring
  - Impact - **Financial** impact of the risk event

What Do We Do With Risk?

- Take the risk
- Avoid the risk
- Accept the risk
- Ignore the risk
- Transfer the risk
- Exploit the risk


Owners
value
wish to minimise
impose
Countermeasures
to reduce
Risk
Threat agents
that increase
to
give rise to
Threats
to
Assets
wish to abuse and/or may damage

How do we measure risk?

- **Threat Agents**- Malicious hacker, Employees, Other Organizations, etc.
- **Threats** – something that can cause harm to an organization. Can be internal or External
  - *DDOS Attack*
  - *Snow storm*

- **Owners**- People within the organization that are responsible for an asset or process
  - *Director of Payroll*
- **Assets** – anything of value to an organization
  - *Web Servers*
  - *Payroll Applications*
- **Counter Measures** – Any controls that are put in place to reduce the threat
  - *MFA*
  - *Privileged Access Management process*

What should we do about risk?

- **Counter Measures** – Any **controls** that are put in place to reduce the threat
  - *MFA*
  - *Privileged Access Management process*

- **Controls** – Put in place to **mitigate** risk

Driving a car

- What risk do we deal with when driving a car?

- How to deal with those risks?
  - *What controls are in place to mitigate those risks?*

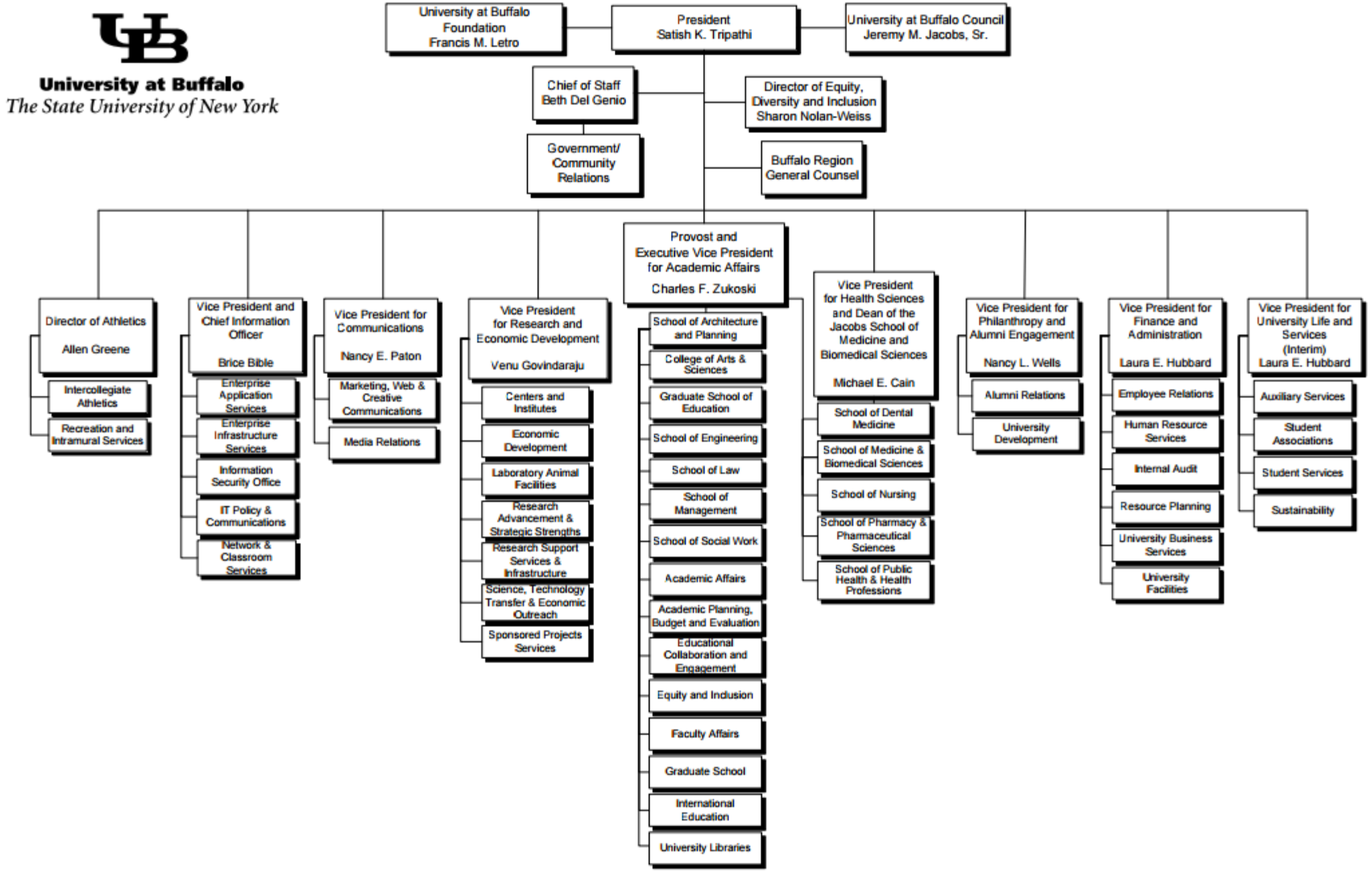
Case Study: University at Buffalo

- Your team (4 people) have been hired by SUNY UB to implement a security framework for various compliance.
- First things first, you will need to setup a risk management plan.
- SUNY UB is a large organization, one of the largest university of the SUNY system. ~30,000 Students; ~6,000 Employees, ~2,500 Faculty, ~$716M Budget, ~12 Schools, ~40 Departments.
- **Let's discuss**

Planning

- Scope & boundary
  - *What are we working within?*
- Resources
  - *What resources do we have at our disposal?*
  - *1 vs 100*
- Criteria
  - *What constitutes a risk to the organization? Is it being measured consistently?*
- Policy
  - *Do we have policy in place?*
- Enforcement
  - *Who will enforce this?*
- Information Classification and Handling
  - *Do we know what we need to protect?*

University at Buffalo
The State University of New York



Last Updated: July 2016

Assets

Inventory

Ownership

Acceptable Use

Impact to the business

Physical Access

Network

User

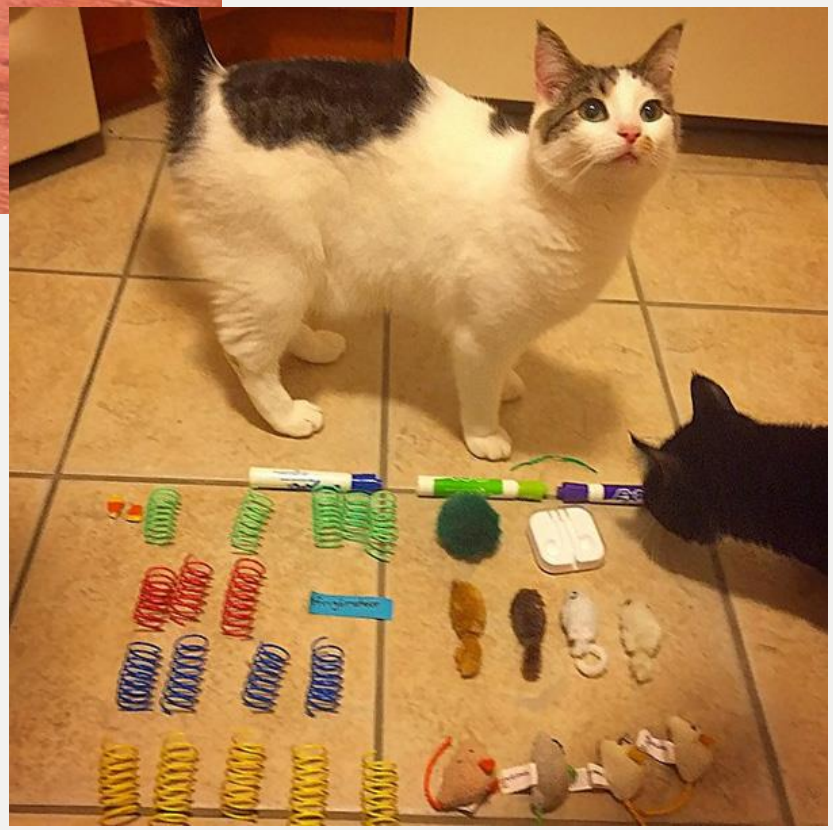
Software

Hardware

Operational

Procedural and Policy

Information and Data



5 Min – Brainstorm what assets UB has + uses

- Quick list of 4-6 assets
  with your group

Mini Case-Study

Active Directory (User Management)	Students' Computers
Exchange (Email)	Wifi
File Servers	UBLearns
Print Servers	Research Assets
VoIP System	Hypervisor (Virtualization)
Network (Switches & Routers)	Classrooms
Workstations	Software
Server Rooms	Sensitive Data/Information
Offices	UBHub

Mini Case-Study

Asset	Asset Inventory & Use
UBHub	- Students' PII, Grades, Schedule - Employee Info - Databases & ODBC - Multiple Privilege & Regular Users
Exchange (Email)	- PII?, Privacy, Grades? - Conversations - Personal & Business - Research - Multiple Privilege & Regular Users
Server Rooms	- Hypervisor (Virtual Machines) - Network Equipment - Users with Physical Access - Data & Info

Threats

- **Internal** to our organization
  - o Budget loss for needed projects
  - o Systems growing overly complex
  - o System failures
  - o Staff turnover
  - o Insider threats
  - o Politics/Agendas
- **External** to our organization
  - o Regulatory
  - o Legal
  - o Environmental / Weather related
  - o Utility related
  - o Natural disasters
  - o Economic
  - o Geo-political
  - o Civil unrest
  - o Cybersecurity events

Vulnerabilities

- Similar to Threats, But within our control
- Weaknesses or gap
- Not just **technical** controls
- Usually specific

- **What is the Likelihood of exploitation?**
- **How can it be exploited?**

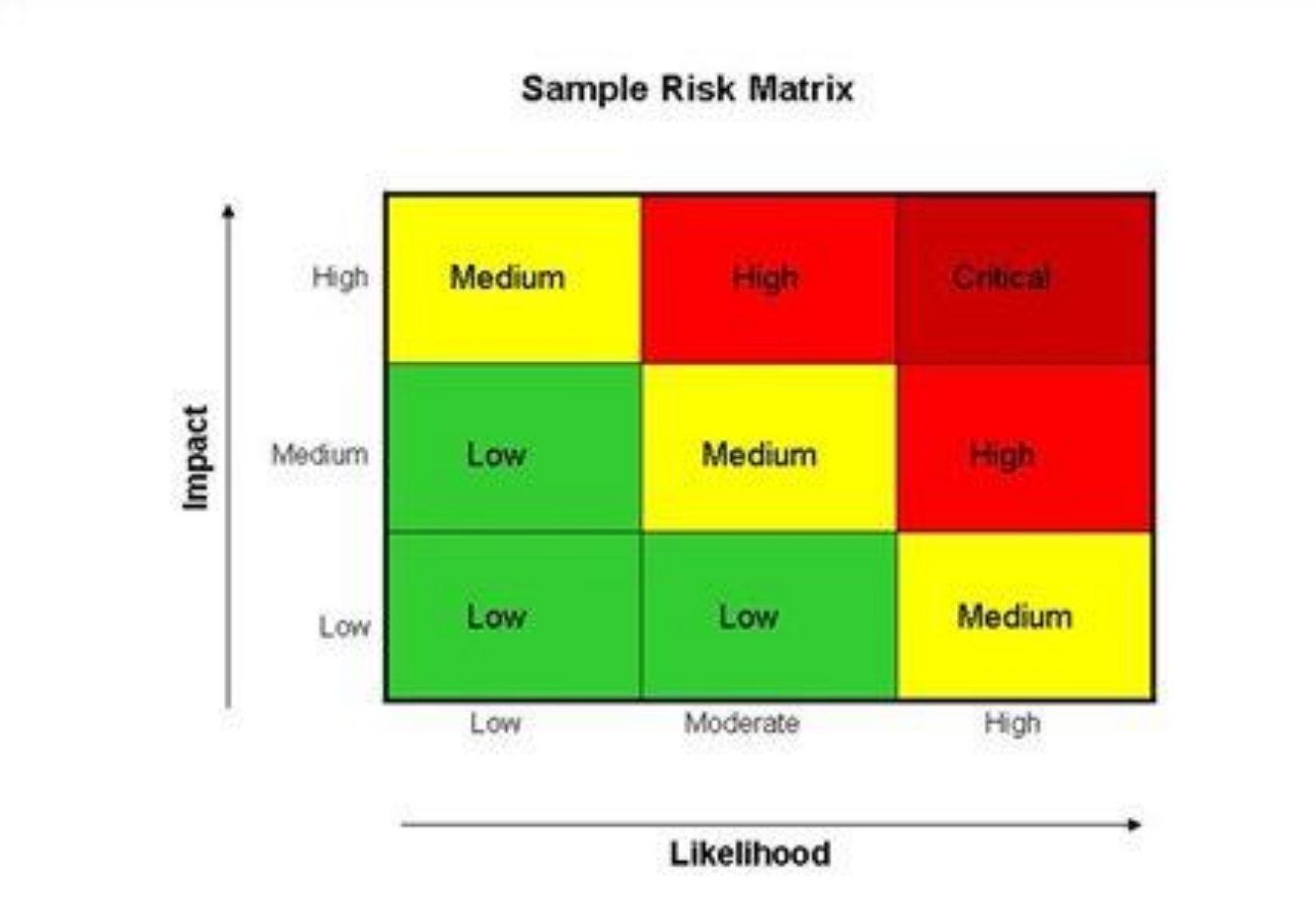
5 min – Brainstorm what threats and vulnerabilities the assets maybe affected by

Threats and Vulnerabilities

Asset	Asset Inventory & Use	Threats	Vulnerabilities
UBHub	- Students' PII, Grades, Schedule - Employee Info - Databases & ODBC - Multiple Privilege & Regular Users	- Failure - Insider Threats - Overly Complex - Regulations and Legal	
Exchange (Email)	- PII, Privacy, Grades - Conversations - Personal & Business - Research - Multiple Privilege & Regular Users	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII
Server Rooms	- Hypervisor (Virtual Machines) - Network Equipment - Physical Access Needed - Data & Info	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation

Risk Identification & Risk Analysis

- Follow consistent criteria and measurements
- Prioritize and plan (risk treatment)
- Risk Register & Matrix
- Impact
- Likelihood
- Security Frameworks



5 min – What is the impact and likelihood of each threat/vulnerabilities?

- Qualitative - Impact + Likelihood
- Quantitative – Using #’s

Qualatative Risk Assesment

Asset	Threats	Vulnerabilities	Impact	Likelihood	Risk
UBHub	- Failure - Insider Threats - Overly Complex - Regulations and Legal	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	Medium	Low	**Medium**
Exchange (Email)	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	Medium	Low	**Medium**
Server Rooms	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	High	Medium	**High**

Quantitative Assessment

Asset	Threats	Vulnerabilities	Impact	Likelihood	Risk
UBHub	- Failure - Insider Threats - Overly Complex - Regulations and Legal	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	$1.5M	3	$4.5M
Exchange (Email)	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	$1M	2	$2M
Server Rooms	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	$3M	6	$18M

Risk Response

Avoid

Mitigate

Transfer/Share

Accept

Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment
UBHub	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	Medium	- Restriction of Users (Least Privilege Principle) - Documentation - Within a year
Exchange (Email)	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	Medium	- Restriction of Users (Least Privilege Principle) - Documentation - Encryption - With two years
Server Rooms	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	High	- Replacement of HVAC and equipment - Documentation - Access Control - Card System - With 6 months

Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment
UBHub	- Too much access	Medium	- Restriction of Users (Least Privilege Principle) - Within a year
	- No Documentation - Lack of Knowledge	Medium	- Documentation - Encryption - With two years
	- Misconfigured	High	- Reconfiguration and Documentation with screenshots - Contact Consultants - Within 6 months

Monitoring Risk

- Yearly reviews/audits
- Change in policies
- New risk assessment criterias
- Change in criminal landscape
- Risk Dashboards
- E-GRC
  - *Governance*
  - *Risk*
  - *Compliance*

5 min – How can we check that our plan is working?

- Brainstorm how we can check that our controls work on an annual basis

Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment	Yearly Check
UBHub	- Too much access	Medium	- Restriction of Users (Least Privilege Principle) - Within a year	- No changes occurred, Possible DATO needed
	- No Documentation - Lack of Knowledge	Medium	- Documentation - Encryption - With two years	- Encryption is in testing environment
	- Misconfigured	High	- Reconfiguration and Documentation with screenshots - Contact Consultants - Within 6 months	- Configured properly, Risk Mitigated

10 min break

Information and Data Classification | Handling and

- At Rest
- In Transit
- Disposal
- Hard Copy
- Electrical Format
- Storage Media

- Public
- Internal
- Departmental
- Confidential/Sensitive
- Highly Restricted

- **Need to Know**
- **Least Privilege**

Regulations And Industry Standards

- What regulations affect our organization?

- HIPAA
- FERPA
- FISMA
- State Laws – NY DFS
- International Laws - GDPR

- What Industry Standards affect our organization?

- PCI – DSS

Security Frameworks

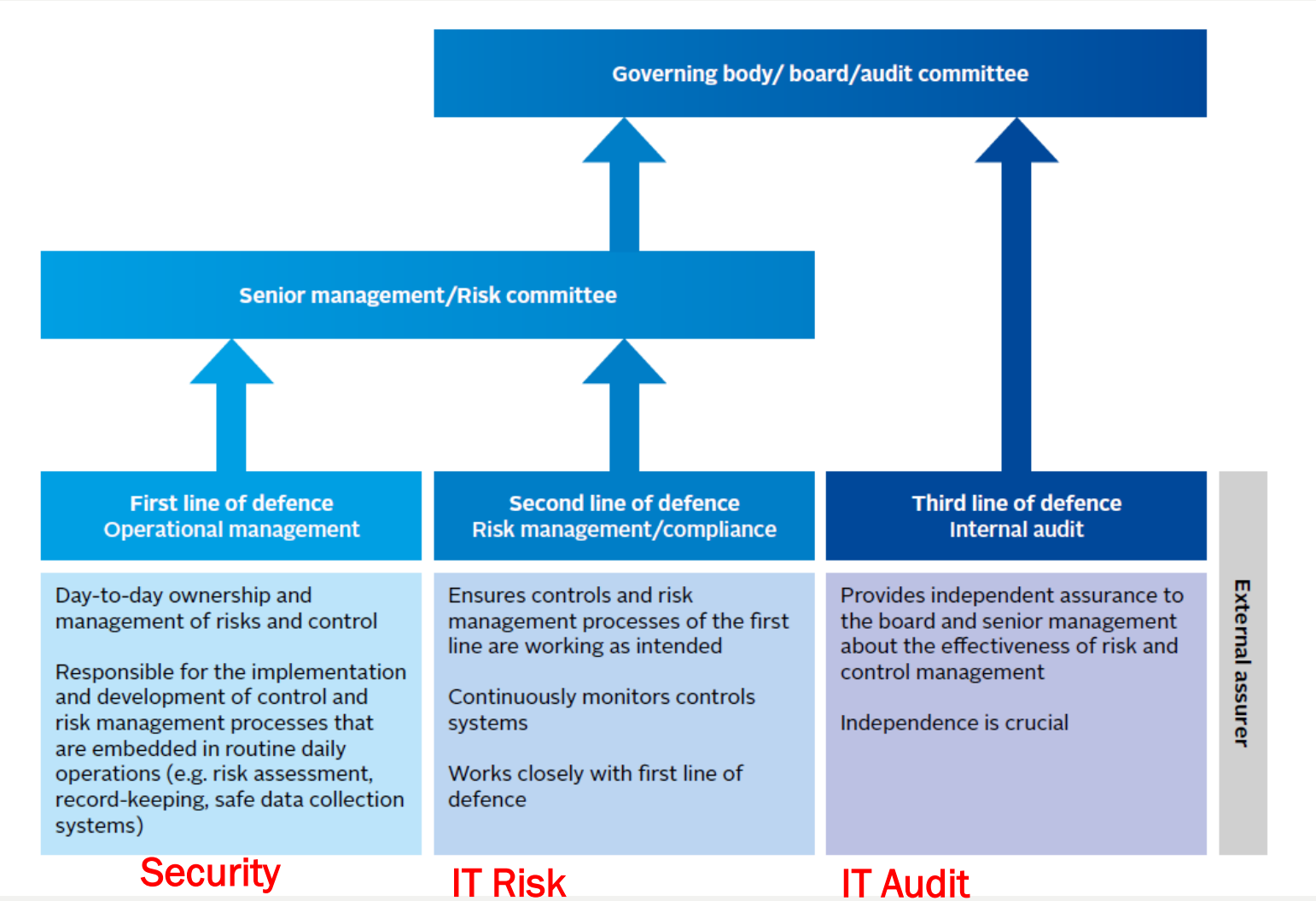
- COBIT
- ISO 27000 Series
  - *27001*
- NIST SP 800 Series
  - *NIST 800-53*
- HiTrust CSF (Current version is 9.1)
  - *Health Care*

What do organizations do with frameworks?

- Frameworks tell organizations what controls should be in place

- Standards + Regulations affect the organization
  - *Frameworks **prescribe** controls to "**Treat**" those Industry Standards + Regulations*

Controls



- **Recommended** by Risk management
- **Assured** by Internal Audit

Risk Management - Summarized

- Planning!
  - *Scope, Boundaries*
- Asset Management
- Threat Identification
- Vulnerability Identification
  - *Auditing and Reviews*
- Risk Assessment
  - *Asset Risk Level*
  - *Threat Risks*
  - *Vulnerability Risks*
- Risk Treatment or Risk Response
- Monitoring
- Security Framework
- Compliance
- Info Handling and Classifications

- Compliance
- Security Frameworks
- Planning
- Asset Management
- Threat Identification
- Risk Assessment
- Vulnerability Identifications
- Risk Treatment & Governance
- Monitoring

- https://www.nist.gov/cyberframework

Demo HiTrust 6.0 – Current Version is 9.1

- Level 1 vs Level 2 vs Level 3
- Control Specification
- Regulatory Factors
- Implementation

References

- https://uspa.org/Find/FAQs/Safety