MGS696 - Tech Consulting for Social Impact

- Develop a system using Salesforce for a local non profit
- Learn to be a consultant
- Undergrads & Grads welcomed!
- Talk to Alex after class

Risk Management

BY ALEXANDER BITAR

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**

What is **risk?**

Risk

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

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

IT 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 – Loss of Revenue
- Vendor Driven – 3rd Party Risk (Target Breach)
- Accidental – Oops I opened a email with ransomware
- Internal – Corporate Espionage, Internal Threats
- Legal – Geopoliticial
- Natural Disasters or Environmental – Nice firewall

How to Calculate Risk: **Impact** x **Likelihood**

- **Impact** - If a threat were to materialize, how could it affect our business?

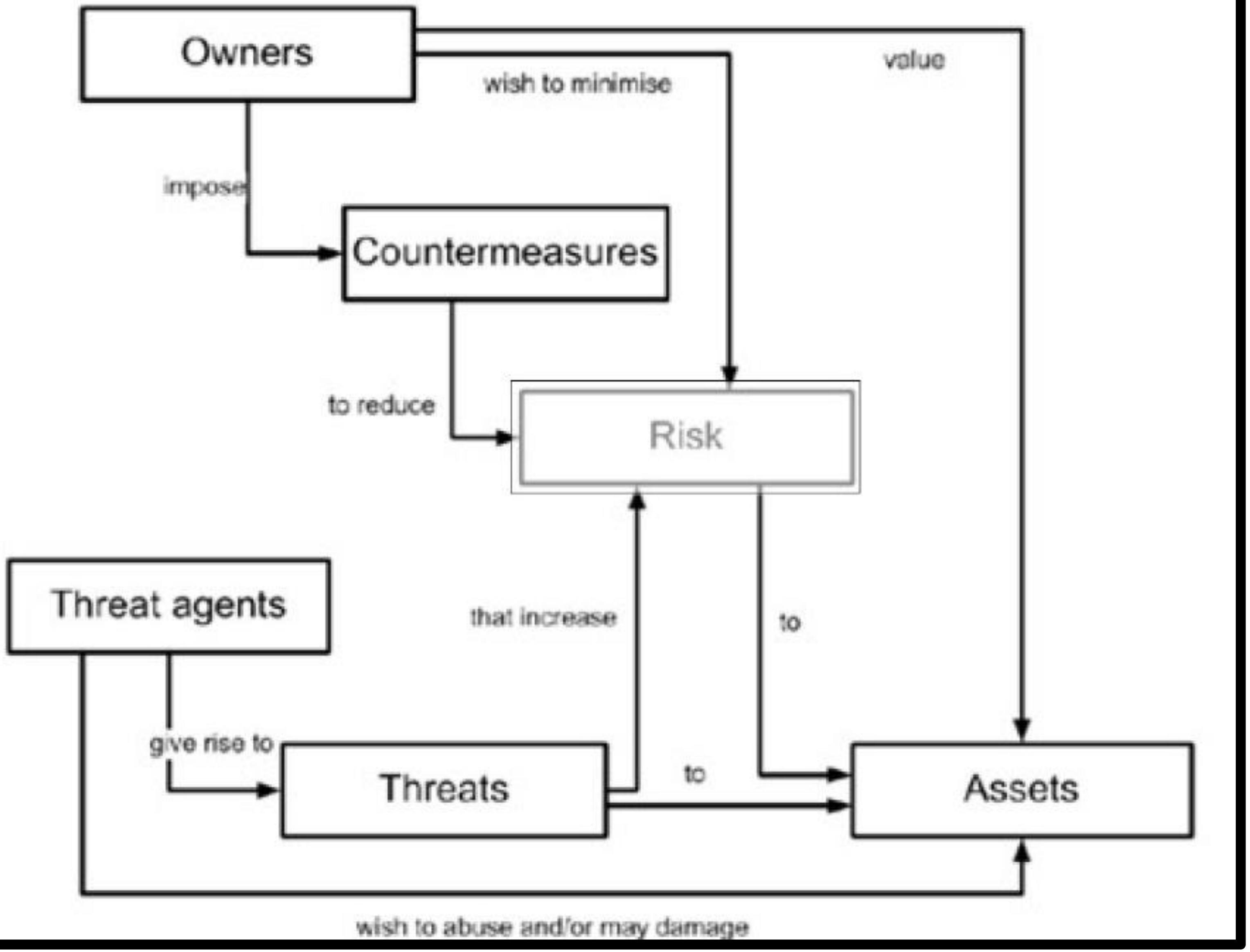
- **Likelihood –**what is the probability of a threat materializing?

- **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
- ******Register the Risk******

ISO/IEC 15408-1:2009(E)



Context:

- **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

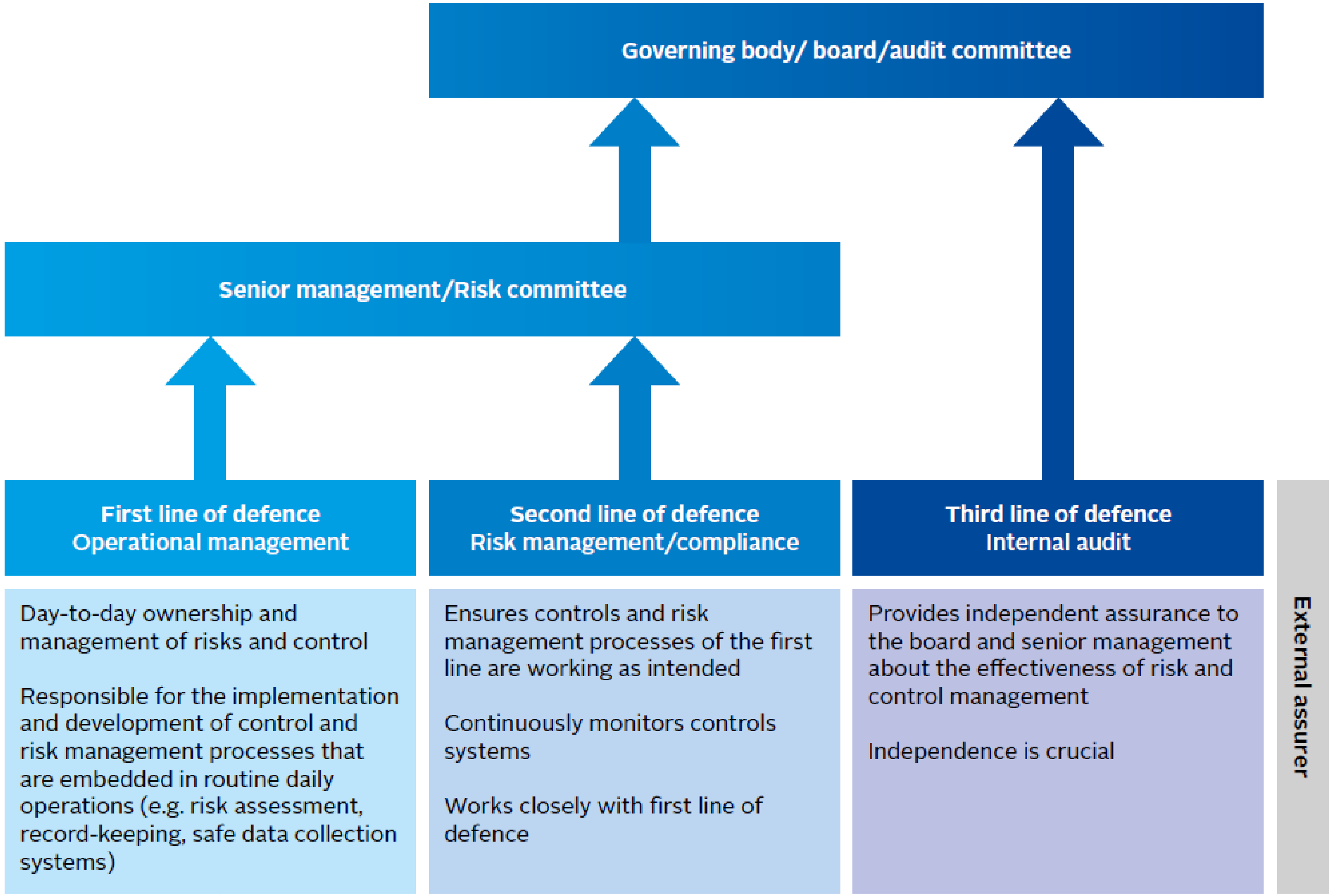
- **Owners**- People within the organization that are responsible for an asset or process
    - Director of Payroll
- **Assets** – anything of value to an organization
    - Web Servers
    - Payroll Applications
- **Counter Measures** – Any controls that are put in place to reduce the threat
    - MFA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

What should we do about risk?

- **Counter Measures** – Any **controls** that are put in place to reduce the threat
  - 2FA/MFA
  - Privileged Access Management process
  - AD Password Policy
  - Inventory List
  - PAM and Normal User list
  - Etc…

- **Controls** – Are put in place to **mitigate** risk

Cybersecurity: 3 Lines of Defense



Governing body/ board/audit committee

Senior management/Risk committee

First line of defence Operational management	Second line of defence Risk management/compliance	Third line of defence Internal audit	External assurer
Day-to-day ownership and management of risks and control Responsible for the implementation and development of control and risk management processes that are embedded in routine daily operations (e.g. risk assessment, record-keeping, safe data collection systems)	Ensures controls and risk management processes of the first line are working as intended Continuously monitors controls systems Works closely with first line of defence	Provides independent assurance to the board and senior management about the effectiveness of risk and control management Independence is crucial	

Security Operations

IT Risk Management

IT Audit Internal Audit

- **Recommended** by Risk management
- **Assured** by Internal Audit
- **3 Lines of Defense**
  - **Sec Ops**
  - **Risk**
  - **Audit**

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

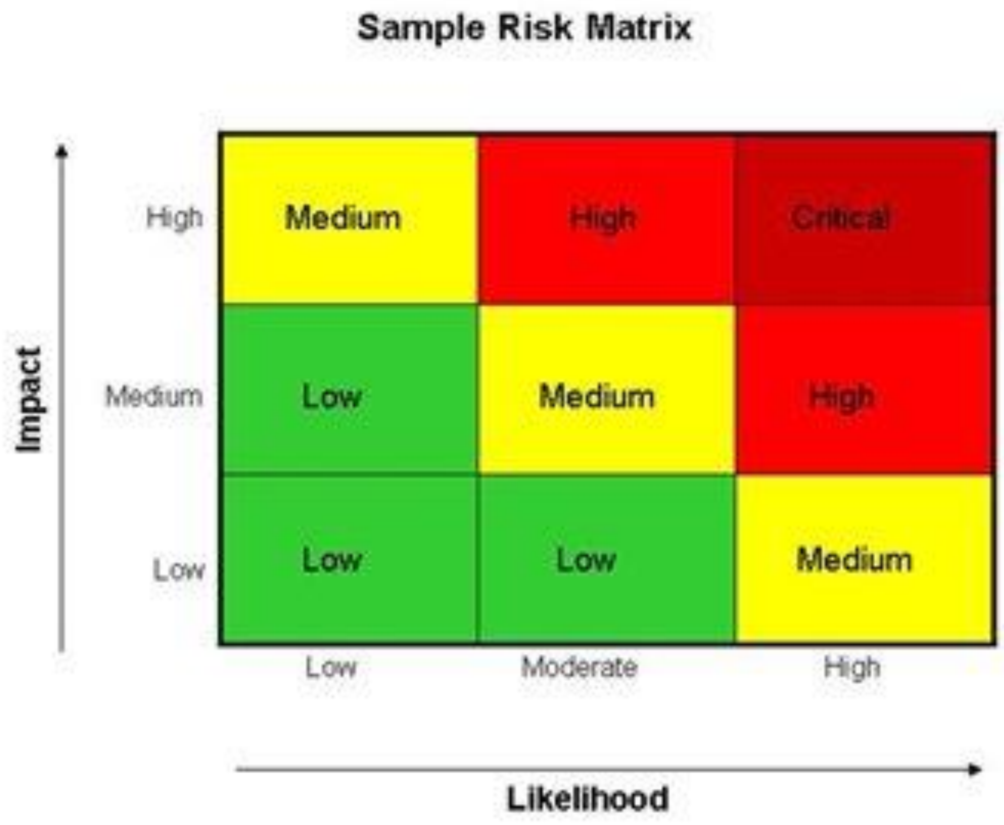
Vulnerabilities

- 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?**

Risk Identification & Risk Analysis

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



Sample Risk Matrix

Impact	Low	Moderate	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium
	Likelihood		

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

Qualitative 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	$1.5M x 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	$1M x 2 = **$2M**
Server Rooms	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	$3M	6	$3M x 6 = **$18M**

Risk Response

Avoid

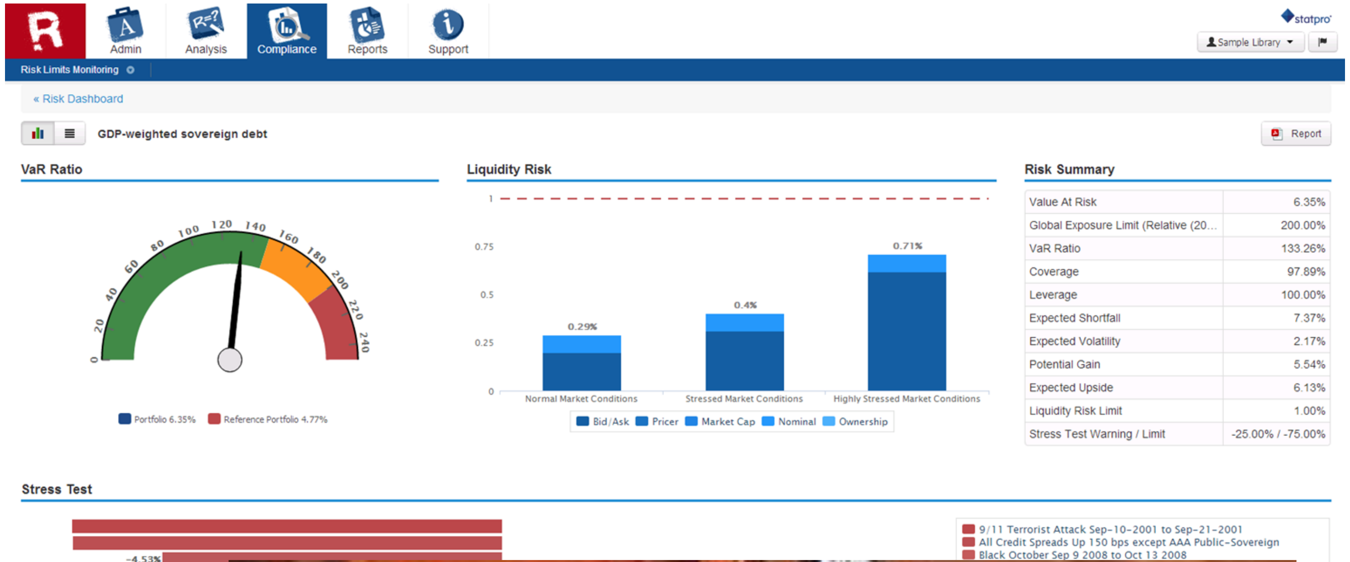
Mitigate

Transfer/Share

Accept

Monitoring Risk

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



Risk Summary

Value At Risk	6.35%
Global Exposure Limit (Relative (20...	200.00%
VaR Ratio	133.26%
Coverage	97.89%
Leverage	100.00%
Expected Shortfall	7.37%
Expected Volatility	2.17%
Potential Gain	5.54%
Expected Upside	6.13%
Liquidity Risk Limit	1.00%
Stress Test Warning / Limit	-25.00% / -75.00%

Information and Data | Handling and Classification

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

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

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

Nano Case Study: Driving a car

- What risk do we deal with when driving a car?
  - Threats?
  - Vulnerabilities?
  - Likelihood?
  - Impact?
  - Response?

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