

# Security Risk Management

---

**Jill Knesek**

**Chief Security Officer**

**BT Americas**



## Definition

---

**Risk management:** a structured approach to managing uncertainty related to a threat.



## Definition – What you tell the CFO

**Risk management:** a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization.



# What it can help you attain

## A Seat at the Boardroom Table



ALE

Optimum  
Organization

Risk  
Appetite

Customer  
Confidence

# Risk Management Terminology

---

<b>Risk</b>	= potential negative event assessed in terms of impact and likelihood of occurrence
<b>Risk Appetite</b>	= level of exposure to risks that an organization is prepared to accept or tolerate
<b>Vulnerability</b>	= asset concentration, expectations, criticality, dependency, exposure, weakness
<b>Controls</b>	= measures in place intended to reduce the vulnerability, likelihood and/or risk impact
<b>Threats</b>	= identified sources of impending disruption, harm, loss or damage e.g. perils, agents
<b>Triggers</b>	= future acts, errors, failures and/or set of circumstances that can cause a risk to occur
<b>Consequences</b>	= sequence of effects due to risk occurrence, assessed up to a specified time horizon
<b>Mitigation</b>	= activities undertaken before or during a risk event to minimise the impact
<b>Impact</b>	= aggregate effect of all the risk consequences, ultimately measured in financial terms
<b>Likelihood</b>	= probability that specified impact occurs (% chance, annual frequency, return period)
<b>Gross Risk</b>	= impact x likelihood, assuming that all controls fail completely, i.e. inherent risk
<b>Net Risk</b>	= impact x likelihood, assuming that all controls work as planned, i.e. residual risk

# Risk Management Fundamentals

---

- Risks are possible future events that could affect business activities and the ability to meet customer expectations.
- Risks are measured in terms of impact on the business (in \$) and likelihood (in %) probability of the specified impact occurring in any given year.
- Impact includes direct financial effects, (such as lost profits, recovery costs, penalties) plus the financial implications of reputation damage, lost opportunities, delays, etc.
- Define risks by describing possible scenarios, with descriptions of current vulnerability, future triggers and the worst credible consequences.
- Risks are managed on a day-to-day basis by a series of controls, and may be further improved by mitigation plans.

# Risk Register

---

- Security risks are operational risks. They form a sub-set of the business risks, which include strategic, financial, regulatory and project risks.
- The Security risk register concentrates on risks that affect the security of business data, compliance with security requirements and the continuity of services.
- Security risks are define by their vulnerability, trigger and consequences
- Risk registers can be created for each line of business, organization, department or geographic region.
- The risk register should include scores or ratings that indicate priority or criticality of the risk. A common scoring system uses numeric scores (1 – 6) which can be defined by numeric values (\$M & %) at Gross, Net and Target levels.

# Sample Security Risks

---

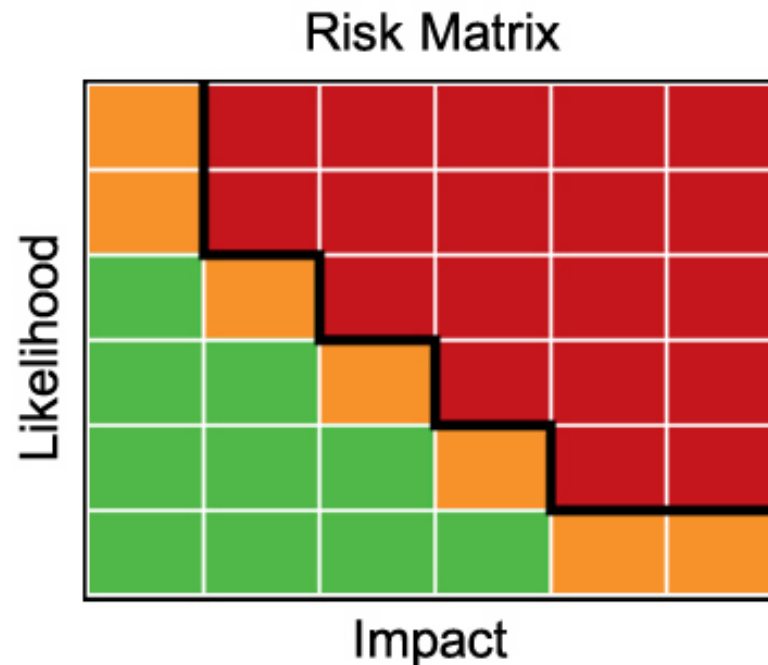
1. **Loss or Theft of Data – proprietary information, personal data, customer bid**
2. **Theft of physical assets - laptops, vehicles, tools, equipment**
3. **Employee malice – fraud, network damage, workplace violence, theft, disclosure, misuse**
4. **Natural disaster – hurricane, flooding, earthquake**
5. **Loss or unavailability of Human Resources – pandemic flu, extreme weather condition, natural disasters**

# Sample Risk Register

No.	Name	Vulnerability	Trigger	Consequences	Likelihood	Impact	Score
1	Loss or Disclosure of data	<b>Vulnerabilities:</b> Proper protection of data that is held on customers, employees and third parties - including intellectual property, personally identifiable information, financial data, etc.	<b>Triggers:</b> 1. Lack of awareness of security policy regarding data protection could result in loss of data 2. Lost or stolen computers 3. A building security breach could result in the theft of data	<b>Consequences:</b> 1. Damage to company's reputation 2. Fines/Penalties 3. Loss of revenue	3	3	9
2	Loss or Theft of Physical Assets	<b>Vulnerabilities:</b> 1.) Inadequate building security 2.) Inadequate access control management	<b>Triggers:</b> 1. Unauthorized access to building 2. Non-compliance with security policy 3. Inadequate site hardening or audits	<b>Consequences:</b> 1.) Financial loss due to the value of equipment. 2.) Fines/Penalties	4	2	8
3	Employee malice	<b>Vulnerabilities:</b> Employee malice could constitute but is not limited to acts of sabotage to network equipment, theft, assault, fraud, industrial espionage, and equipment misuse.	<b>Triggers:</b> 1.) Insecure physical workplace. 2.) Lack of awareness of security policies and personal safety. 3.) Disgruntled employee 4.) Personnel committing internal fraud related to time & attendance, expense reporting, equipment misuse, etc.	<b>Consequences:</b> Failure to adequately educate and protect against physical harm, network sabotage, and fraud can result in low morale, revenue loss, civil litigation, and a negative impact on company reputation.	5	1	5

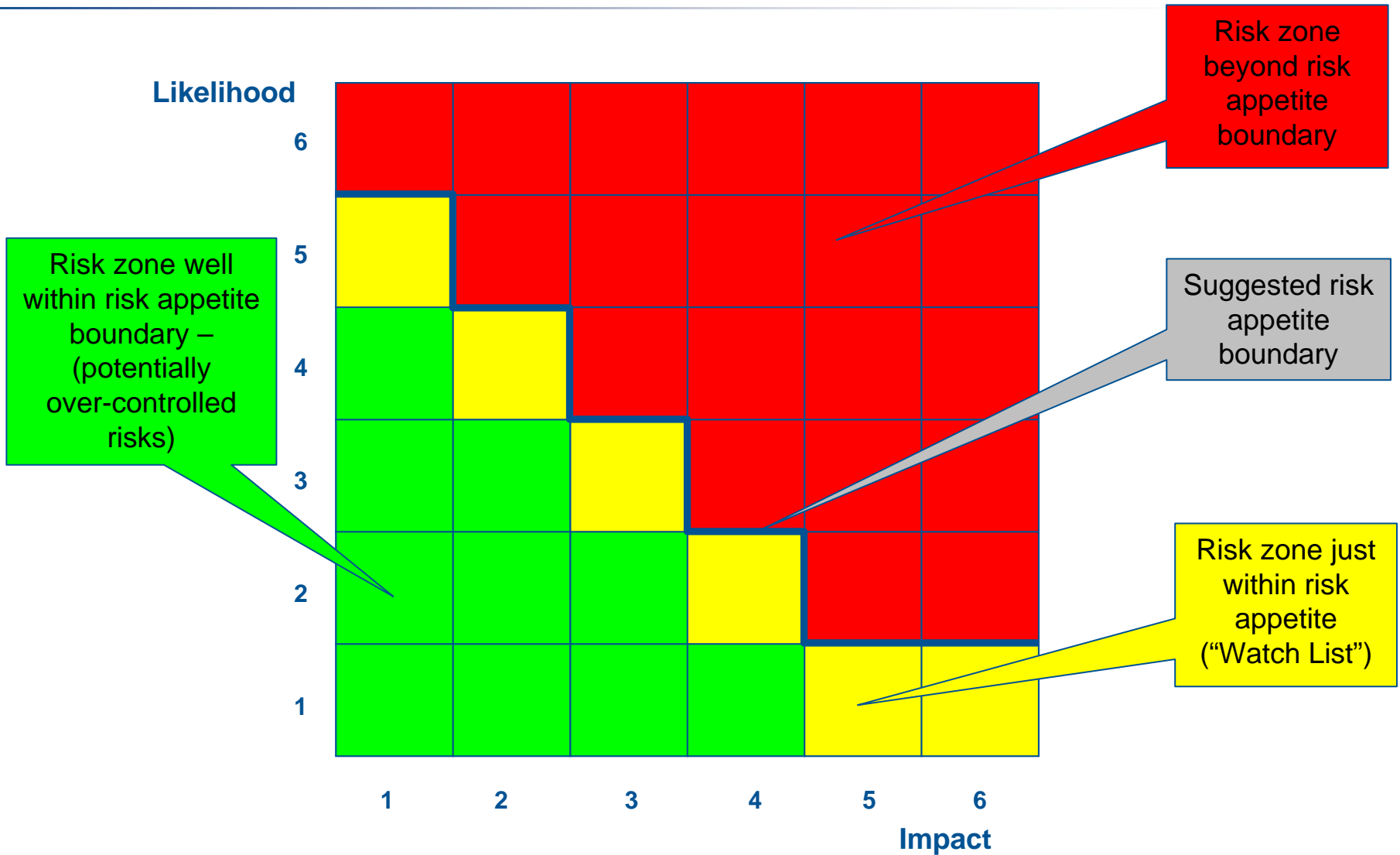
# Risk Matrix

A graphical mechanism for illustrating a single risk, a family of risks or an entire risk register to show the relative impact vs. likelihood.

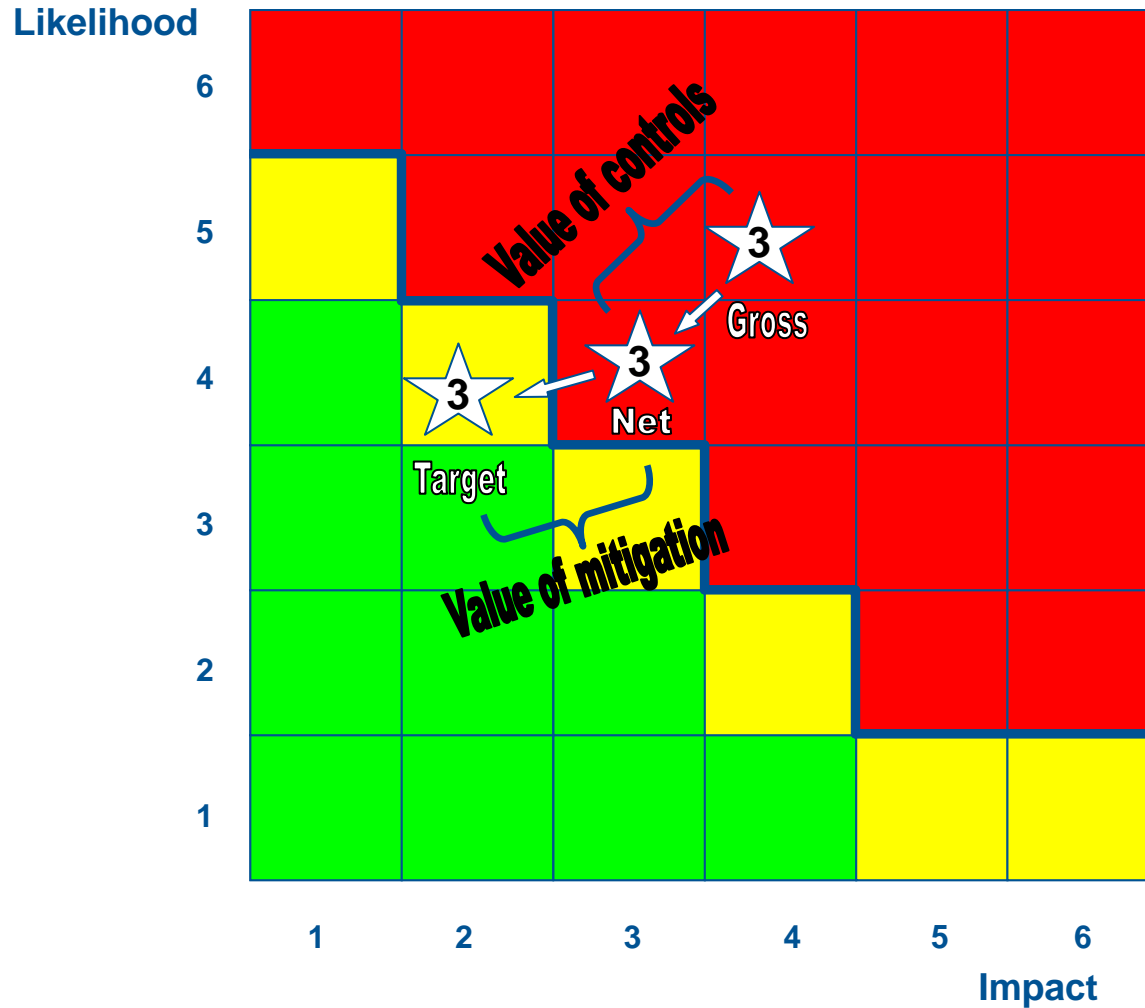


The dark black line indicates a company's risk appetite

# Cost effective management – Using the risk matrix



# Defining Security Projects and Measuring ROI



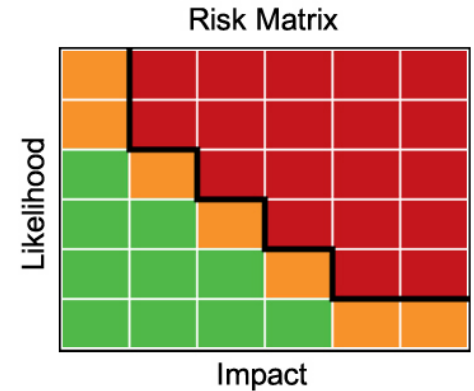
# Risk Program Maturity

---

- As a Risk program becomes more mature your data becomes more accurate and your risk register better aligned to reality.
- Historical data does provide a better understanding and rating of future risks
- Ensure you are collecting the right data to help you better define your risk register.
- Use actuals to guide your security strategy and projects
- Use actuals to obtain budget for new security activities that further mitigate risk.
- Use actuals to create an Annual Loss Expectancy (ALE)

# Value of a Risk Management Program

- The umbrella program driving all of your other security programs
- If there is no risk you don't need security
- Align security with the business strategy
- Properly apply resources based on risk
- Divert budget/resources from low risk areas to high risk areas
- Learn to speak the business language



# Ensure a Seat at the Boardroom Table

Learn to speak the business language.



Thank you!