



ISACA Edmonton Chapter – IT ORM

IT Operational Risk Management

**ISACA Edmonton Chapter
Breakfast Meeting March 8, 2007**

Agenda

- Definitions: Risk, Operational Risk Management, IT Operational Risk Management
- IT-ORM: Why do it?
- Whose Responsibility?
- IT Risk Analysis – NIST Methodology
- Mapping ORM to COBIT
- Other Methodologies
 - ISF IRAM/FIRM, OCTAVE, RCMP, NIST, BS7799-3/ISO-IEC27005
- Key Messages for IT-ORM
- Concluding Thoughts
- Q&A

PLEASE RESPECT ALL COPYRIGHTS

Dedication

In memory of the late **Robert J. Garigue**, a visionary, and a passionate advocate of information security, who passed away on January 10, 2007. Mr. Garigue was most recently VP for Information Integrity and Chief Security Executive for Bell Canada.



*Some compare risk limits to brakes on a car, and worry that they will slow down a business. But while brakes do allow a car to slow down or stop when it needs to, they also give the driver the confidence to go even faster (e.g., race cars have the best brakes). **For operational risk, having good brakes means setting performance goals and limits for each operational risk area and instituting regular reviews to ensure appropriate decisions and actions.***

Risk Defined

- Risk is the ***exposure to a proposition, the outcome of which one is uncertain***
- Risk has two components: ***uncertainty***, and ***exposure***.

IT Risk may be defined as:

- The **likelihood** that particular **IT vulnerabilities** will be exploited by specific **threats**, which could result in undesirable **consequences**.

Consequences of Risk

The consequences of risk are expressed in terms of ***severity and probability***.

The consequences could be:

- Harm to people;
- Loss of an asset, a service or function;
- Loss of confidence and/or trust;
- Unauthorized access, or damage, to data & information
- Legal or regulatory exposure;
- Direct financial losses (loss of business/productivity, remediation costs); and/or,
- Indirect financial losses, such as through loss of confidence or trust.

Options for Risk Treatment

- **Avoid**
 - *Not an option in many cases*
- **Accept**
 - *To satisfactorily accept risk, it needs to be formally accepted, by the appropriate level/s of authority*
- **Transfer**
 - *“Cybersecurity Insurance” - Insure against losses*
- **Mitigate**
 - *Suitable & cost-effective controls & safeguards to reduce exposure, probability and/or impacts*

Types of IT Risk Management

- **Strategic Risk Management**

- Defines an organization's strategy for managing risk

- **Tactical Risk Management**

- Pertains to “finites”, such as project risk management for an initiative (e.g., development of an eCommerce application), or to address a specific exposure in an information system
- A specific approach or initiative to address a particular risk

- **Operational Risk Management**

- Day-to-day operations, such as once the (example) eCommerce system is in production mode
- It is linear, open-ended, not finite

Definition – (IT) Operational Risk

*“**Operational Risk** is defined as the risk of **loss** resulting from inadequate or failed internal processes, people and systems or from external events.”*

Basel II

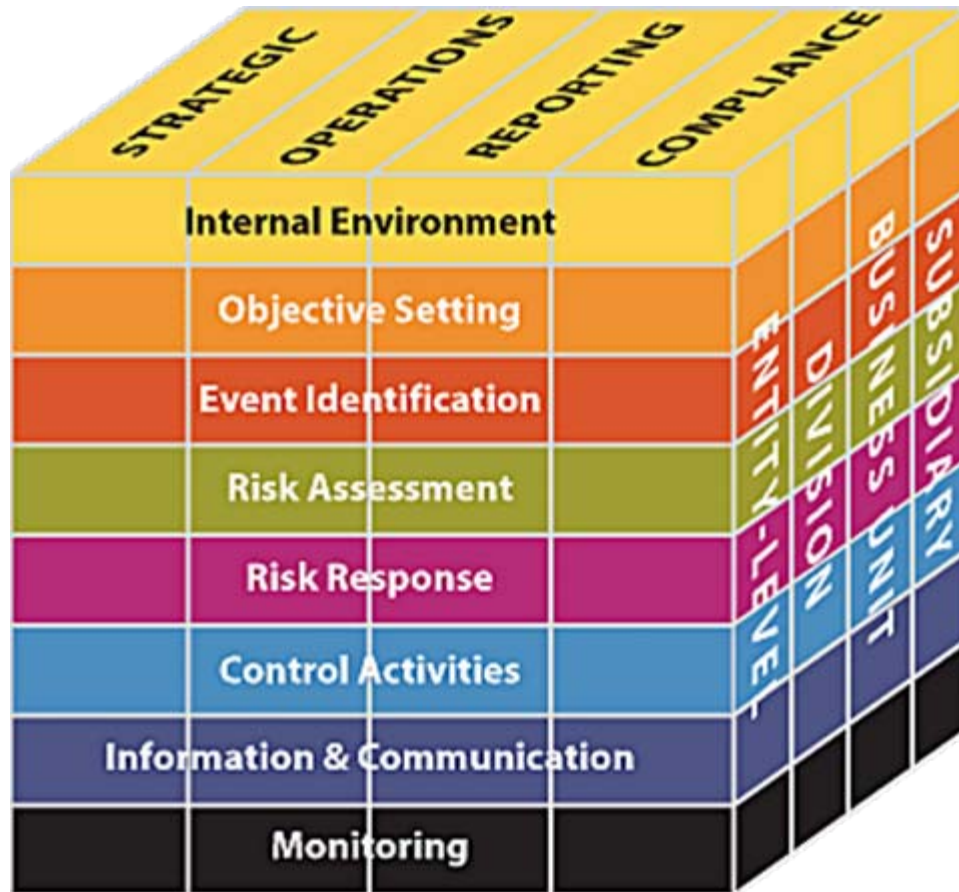
Operational Risk Management Defined

- Thus, Operational Risk Management (ORM) is the *oversight and management of many forms of day-to-day operational risks including the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.*
- The term “operational risk” is rarely assigned a specific definition, rather a list of functional areas and processes are associated with it. Examples include:
 - **Information Technology**
 - Business Continuity
 - Human Resources; and,
 - Legal Risk.
- **Operational Risk goes across the entire organization**

Operational Risk Management is a Journey - Not a Destination



COSO Enterprise Risk Management (ERM) Framework



Source: WWW.COSO.ORG

IT (Operational) Risk Management

The process concerned with the *identification, measurement, control and minimization* of security risks in information systems to a level commensurate with the value of the assets protected.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Dimensions of IT Operational Risk Management

- **People**

- *Internal Users: Employees, Contractors (fraud)*
- *External Users: Partners, Customers*
- *Unauthorized Externals: Criminals, vandals (fraud, theft)*

- **Processes**

- *Execution, delivery and process management*
- *Employment practices & workplace safety*
- *Clients, products, and business practices*

- **Technology**

- *Business disruption & systems failure*
- *Secure product delivery channels*

- **External Factors**

- *Legislative and regulatory requirements (Privacy, CSOX)*
- *Trust*
- *Reputation*

Why should we bother with IT-ORM?

- Most business processes today are dependent on IT to some degree
- In an operational setting, there is a large number of possible events that could adversely impact IT, and therefore, the business
- The consequences of failures in IT can disrupt the business processes and directly impact the organization, **or the people associated with it**
- Un-managed changes to IT can cause major outages (internal threats)
- The trend in **computer crime** has shifted increasingly from vandalism to *for-profit malfeasance* (external & internal threats)

The strategy for employing the army is not to rely on their [the enemy] not coming, but to depend on us having the means to await them. Do not rely on them not attacking, but depend on us having an unassailable position.

Sun-Tzu, The Art of War

Who is Responsible for IT-ORM?

- **IT Risk Management needs to be appropriately governed: through policy, strategy, and assignment of roles & responsibilities**
- **Because an IT exposure can impact the whole organization, IT-ORM must be integrated into overall Enterprise Risk Management**
- **If (Accountability = Responsibility + Authority), then the **ultimate accountability** for risk management rests with the Board and senior management (CEO, CFO)**
- ***In the absence of formally defined governance, the CIO (and her reports) is typically seen as being responsible for IT-ORM***

Reference Sources:

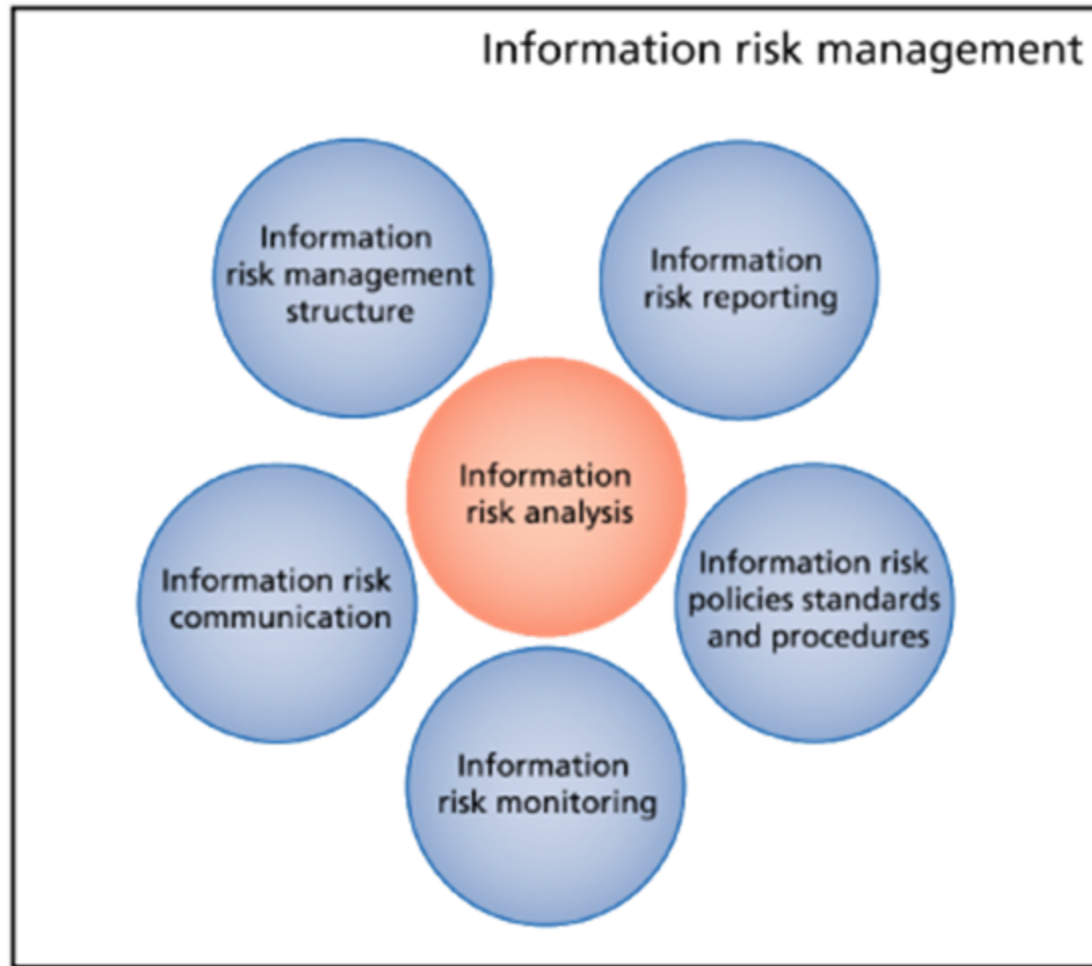
1. The New CIO Leader, Marianne Broadbent & Ellen S. Kitzis, Harvard Business School Press
2. IT Governance Institute publication, “Information Risks: Whose business Are They?”

How do we address IT-ORM?

Through **systematic operational risk analysis.**

Risk Analysis provides the basis for identifying security risks and determining how risks should be managed, through the selection of appropriate risk treatment options.

Elements of Effective Information Risk Management



Source: *Information Security Forum*

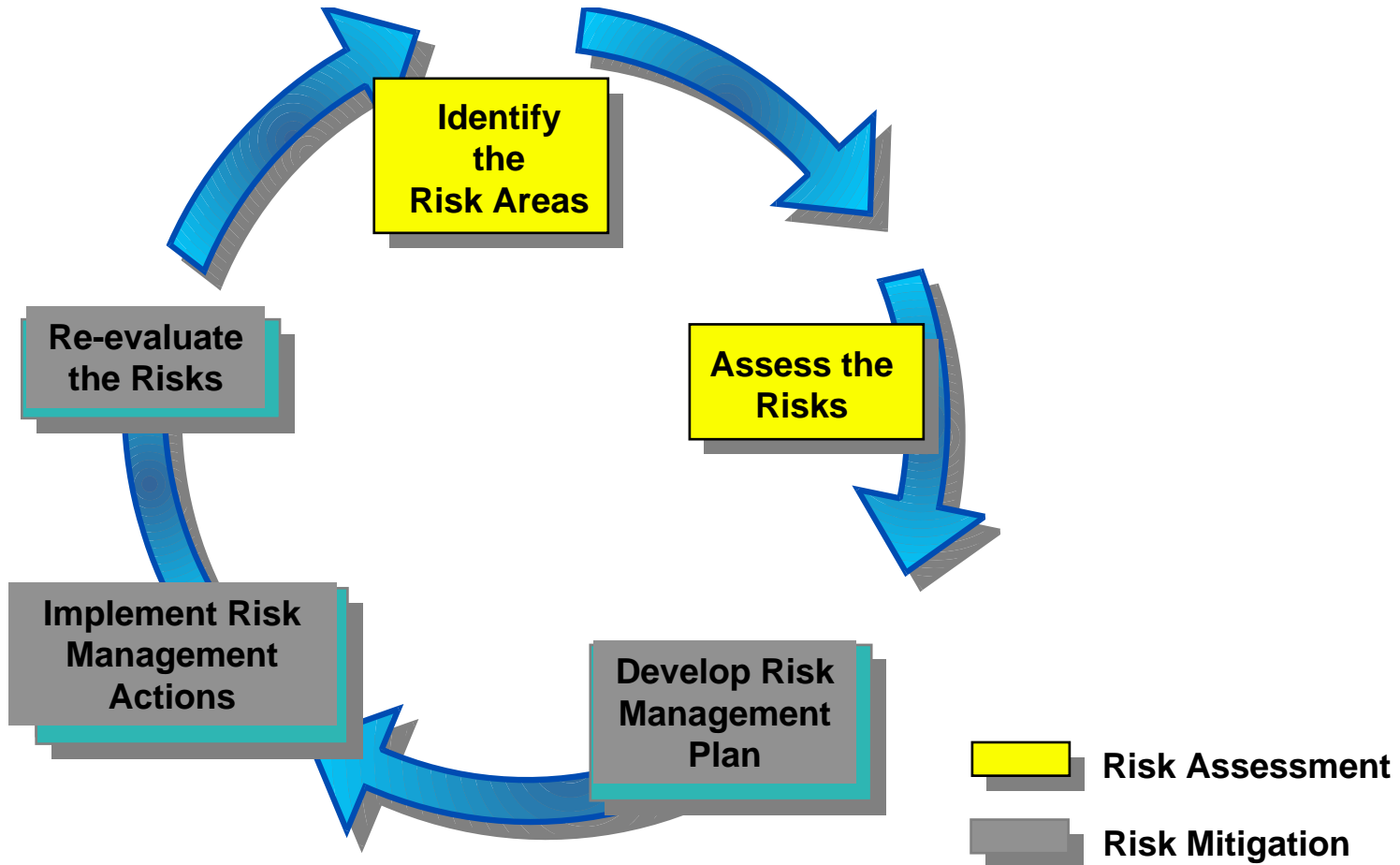
Principles of Operational Risk Management

1. **Anticipate and manage risks by planning**
2. **Accept risk when the benefit is greater than the risk**
3. **Do not accept any unnecessary risk**
4. **Make risk decisions at the right level**

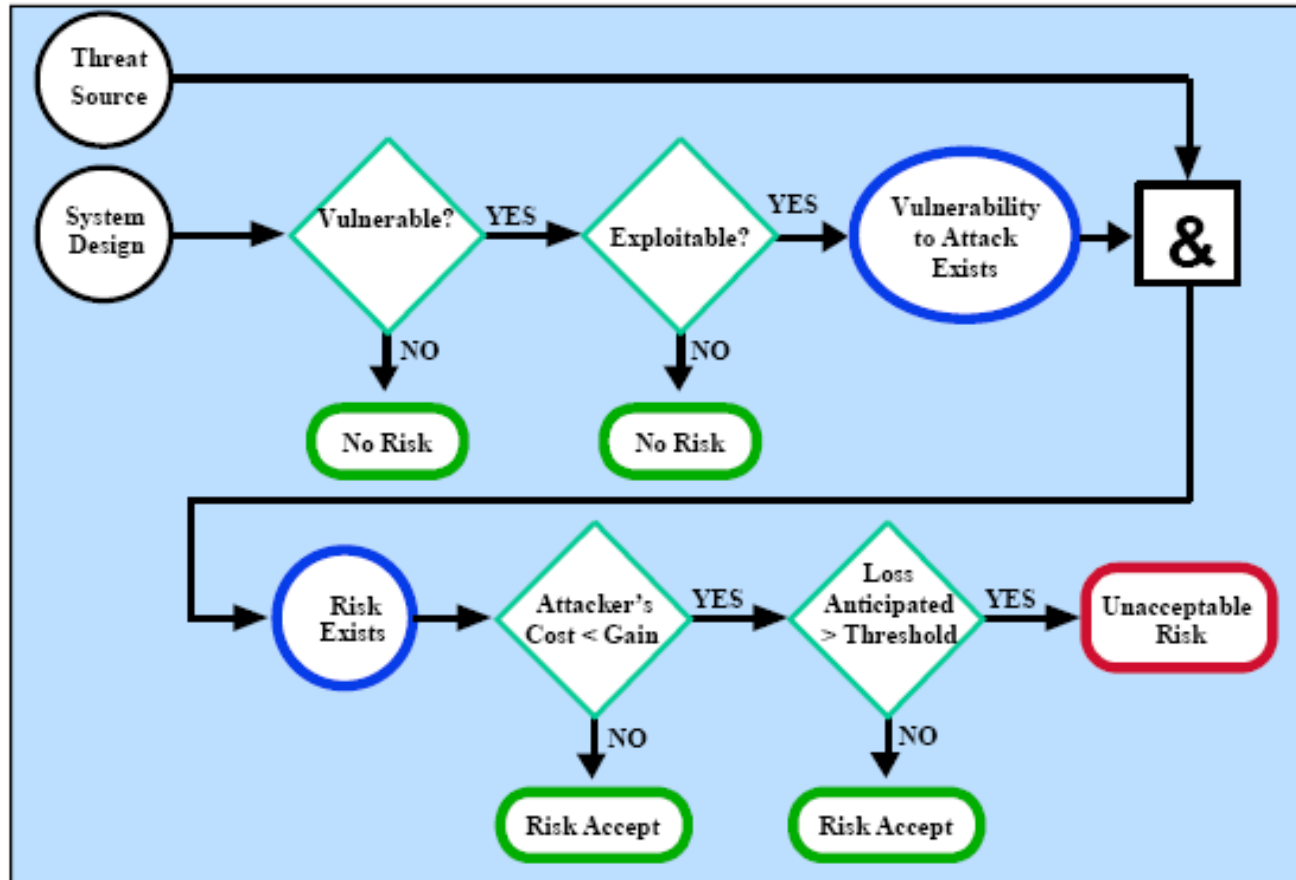
Examples of IT Operational Risk Criteria

- Data Centre environmental controls
- Continuity & quality of electrical power
- Access to data media (storage, in-transit, disposal)
- Electronic Data Interchanges
- Operating systems & application software vulnerabilities (“*patching*”)
- Physical security of workstations, laptops, PDA’s
- Network perimeter security
- Communications and technical failures
- IT processes and procedures
- Security Incident Detection, Response & Management

Risk Management Cycle

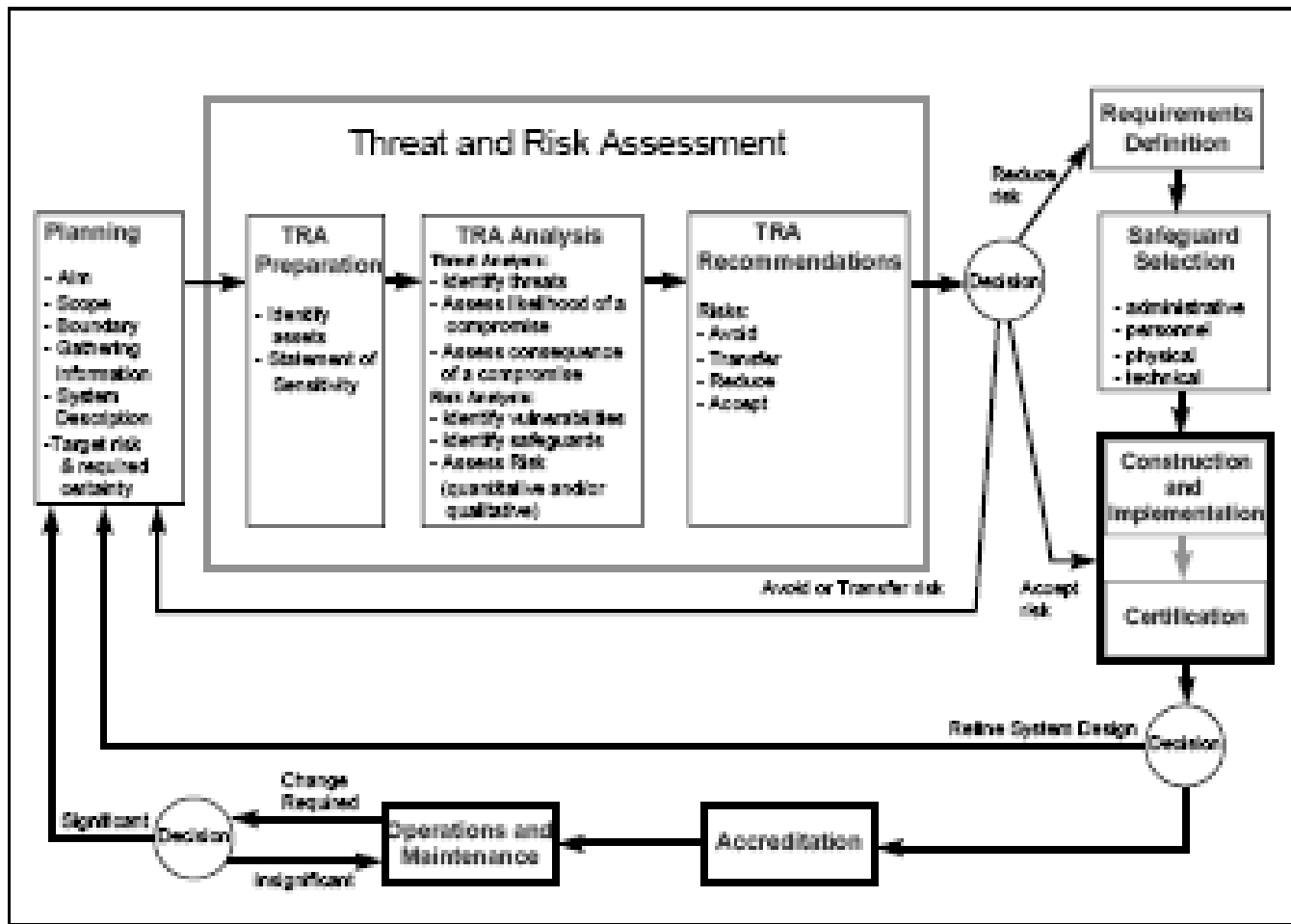


A Simplistic Risk Determination Model



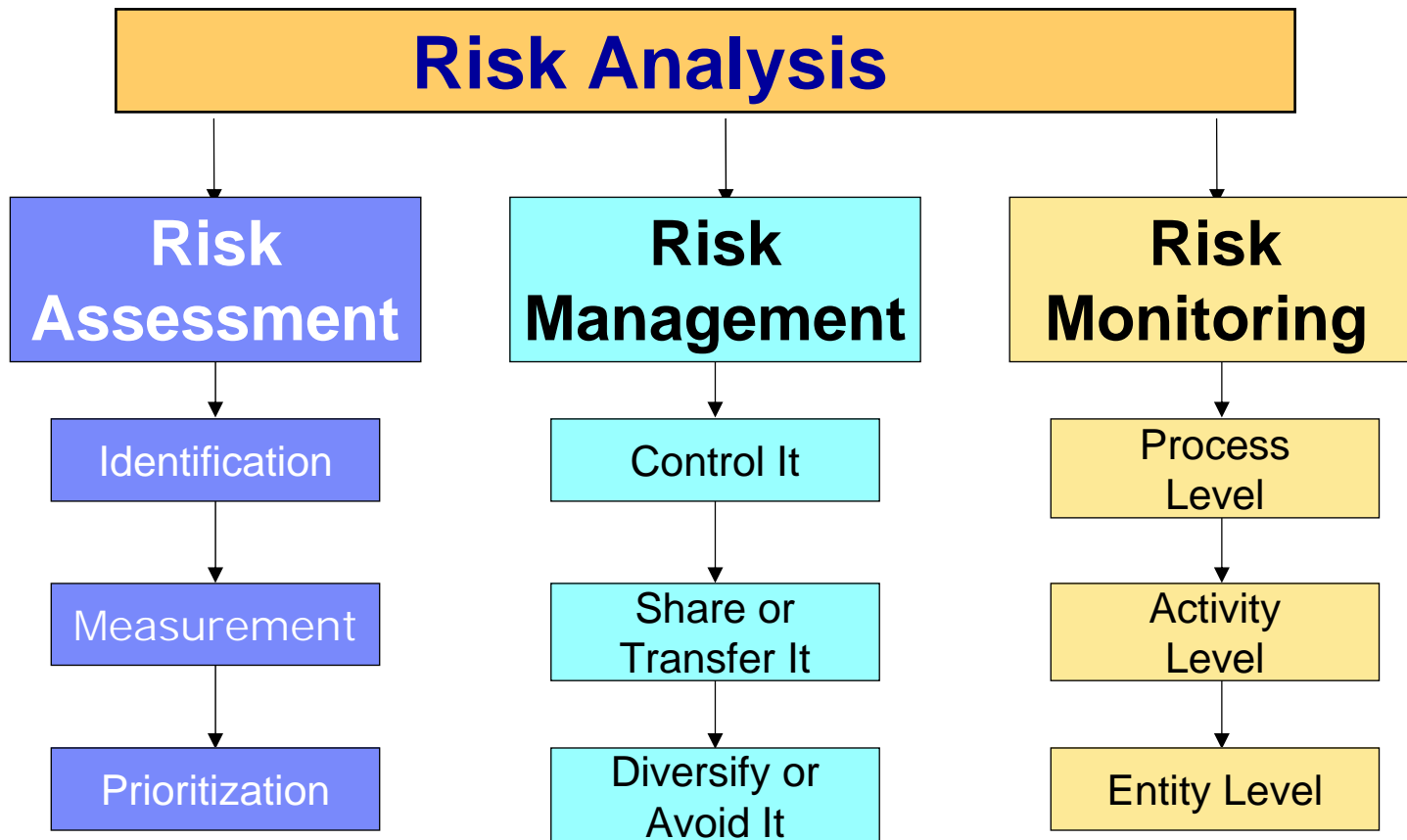
Source: NIST SP800-30

A Risk Management Model



Source: Govt of Canada, Communications Security Establishment,

COSO Approach for Risk Analysis



A Pre-requisite to Risk Analysis

- **Identify the Scope of the Risk Analysis**
- **Know & classify the valuables**
 - Sensitivity
 - Criticality
- **Know your valuables**
 - Exposures and vulnerabilities

In other words, ***know what is at risk***

Quantitative or Qualitative Risk Analysis?

- There are simply not enough data to facilitate purely quantitative risk analyses
 - *Single Loss Event (SLE), Annual Loss Event (ALE)*
- It is possible to estimate costs to remediate (person-hours, materials), but business losses and intangible costs are difficult to estimate
- Involving “business owners” may help
- Use a hybrid of qualitative and quantitative analysis where feasible.

The Risk Analysis Process

1. **System Characterization**
2. **Threat Identification**
3. **Vulnerability Identification**
4. **Control Analysis**
5. **Likelihood Determination**
6. **Impact Analysis**
7. **Risk Determination**
8. **Control Recommendations**
9. **Results Documentation**

Source: NIST SP800-30

- **Risk (Treatment) Decisions**
- **Implement Risk Treatment Measures**
- **Risk Monitoring**

Characterize the System / Environment

- **Hardware**
- **Software**
- **System interfaces**
- **Data and information (sensitivity)**
- **People (administrators, users)**
- **System mission (criticality)**

Assess Risk – Identify Threat Vectors

- ***Internal Threat Vectors (network and non-network based)***
 - System Administrators
 - Disgruntled employees
 - Uninformed employees
 - Contractors and service providers
- ***External Threat Vectors (network and non-network based)***
 - Cyber-criminals
 - Vandals
 - Opportunists
 - Network connected business partners
- ***Force majeure***
 - Electrical power failures
 - Natural disasters

Assess Risk - Identify Threats

- Network hacking
- Social engineering
- System intrusion
- Unauthorized system access
- Unauthorized data access or disclosure
- Fraud
- Data “leakage”
- Data destruction
- Network “eavesdropping”
- System sabotage (“backdoors”, logic bombs)
- System outage
- Loss of communications capabilities
- Business disruption
- Excessive user privileges
- Procedure / process by-passing

Identify Vulnerabilities

Sources

- Results of Threat & Risk Assessments
- Internal & External Audit Reports
- Compliance requirements
- Security requirements
- Vulnerability Test Results
- Vendor advisories
- National Vulnerability Database (e.g., *icat.nist.org*, *nvd.nist.gov*)
- System Design documentation
- Business & IT Process Reviews

Threat & Vulnerability Pairs

Identifying Vulnerability/Threat pairs **assists with projecting the impact**

Vulnerability	Threat Vector	Threat Action
User accounts are not re-validated periodically; terminated user accounts are not disabled	Terminated Employees	Gaining unauthorized access to organizational systems
Network traffic is not encrypted	Unauthorized users (e.g., hackers, terminated employees, cyber-criminals, vandals)	Network can be “sniffed” to obtain more sensitive information (privileged user accounts & passwords)
Data centre equipment does not have backup power	Unplanned power outage	Critical services will be unavailable; Sensitive equipment and/or data could be destroyed

Control Analysis

- **Technical and non-technical**

- *Network security controls*
- *Intrusion Detection & Prevention Systems*
- *User Profiles*
- *Hardening and patching*
- *User Provisioning processes (Add, Change, Delete)*
- *Change Management procedures*
- *Configuration Management*

- **Current Controls and Safeguards**

- **Planned Controls and Safeguards**

- **Assess adequacy of controls & control strategy**

- *To avoid group-think, or overly-subjective assessments, consider consensus-building methods (such as Rand Corporation's Delphi method)*

Likelihood Determination

- **Motivation of Threat Vector (profit, mischief)**
- **Threat Capacity (required expertise)**
- **Adequacy of existing controls**

Likelihood Ratings:

HIGH – The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

MEDIUM – The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

LOW - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis

- **Loss of Integrity**
- **Loss of Confidentiality**
- **Loss of Availability**

Impact Ratings

HIGH - Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.

MEDIUM - Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.

LOW - Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Risk Determination

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)⁸

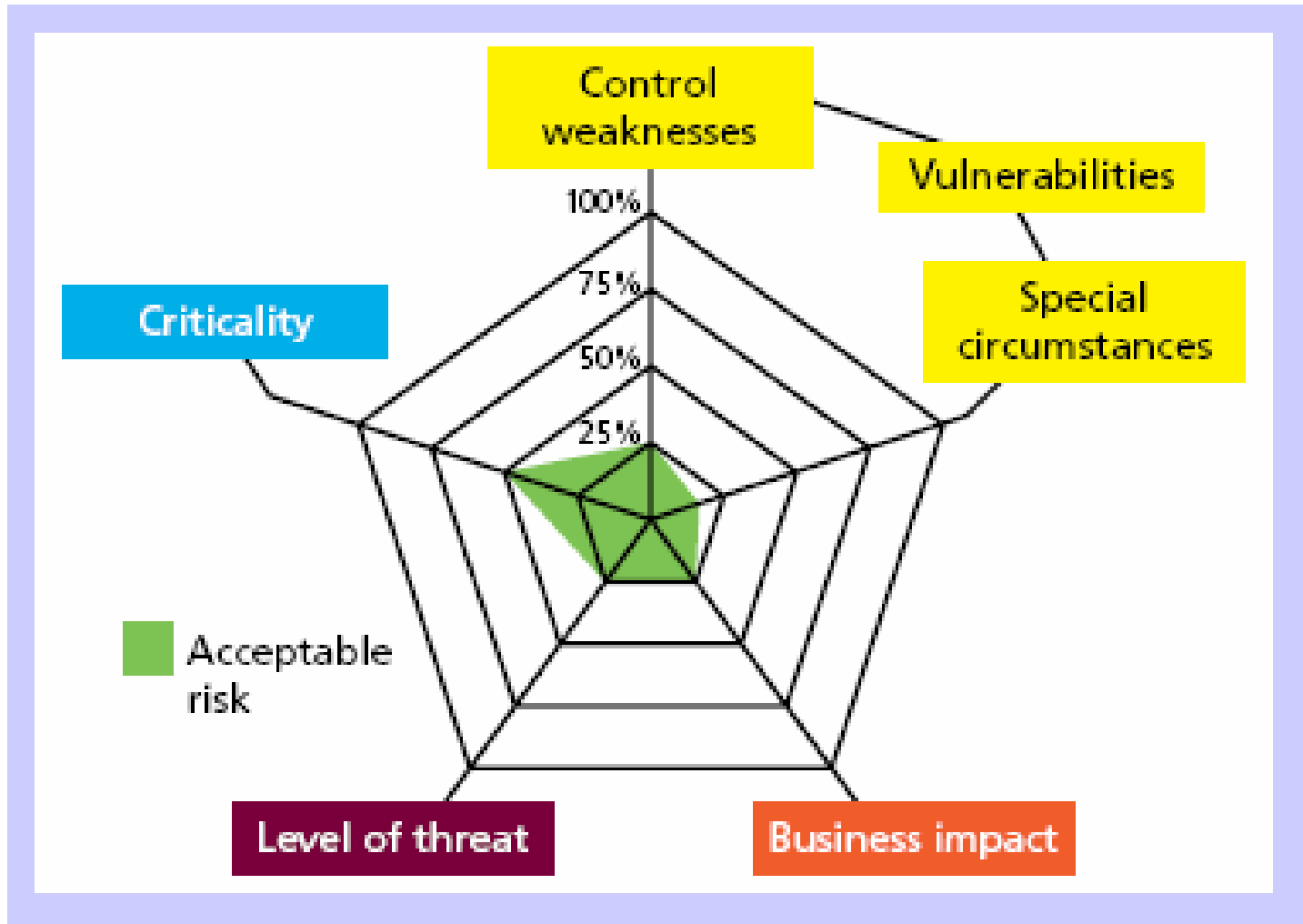
Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Document the Results

Threat Vector	Threat	Existing Safeguards/ Vulnerabilities	Impact	Likelihood	RISK
Internal User (IT Admin)	Unauthorized Changes to Network Configuration could cause major unplanned outages	Weak /Non-existent Change Management; Admin activities not logged; network not monitored	HIGH (could expose the internal network to unauthorized external access)	HIGH	HIGH
Internal User (Marketing Dept)	Unauthorized disclosure of personal customer information	Marketing Department not part of Security (Risk) Council	HIGH (Privacy Breach)	MEDIUM	MEDIUM
External	Network eavesdropping	Encrypted network communications	HIGH (Sensitive information could be obtained, and later used to access systems)	LOW	LOW
Force Majeure (Flooding)	Locale prone to flooding; risk of water damage to Data Centre	Data Centre & equipment location; flood sensors	HIGH (critical systems may become unavailable, or severely damaged)	HIGH	HIGH

Source: NIST SP800-30

Present Risk Analysis Results – An Example

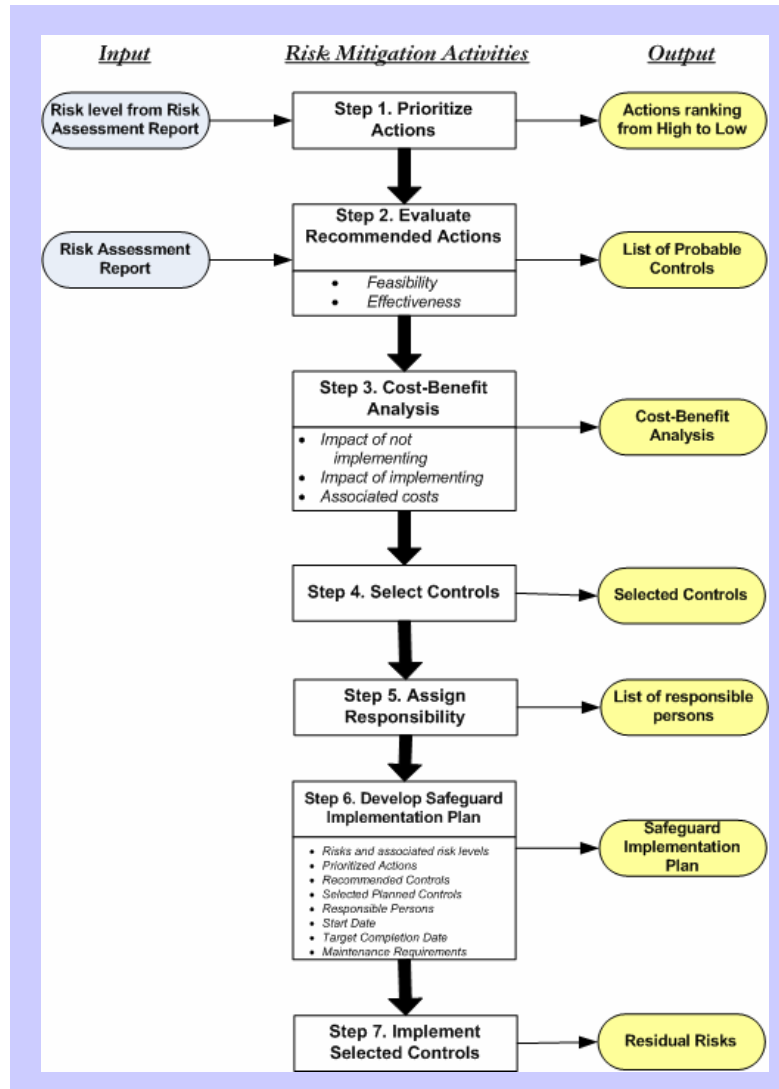


Source: Information Security Forum

Risk Treatment

- **Is the Risk Acceptable?**
- **If not, what are the options to mitigate risk?**
- **Establish priority**
- **Evaluate Risk Control options (include Cost-Benefit Analysis).**
Examples:
 - *Implement Formal Change Management*
 - *Implement (ITIL/ITSM) Change Management*
 - *Implement tool to log, monitor and audit Administrator activities*
 - *Ignore*
- **Will there be any residual risk?**
 - *Is the residual risk acceptable?*
- **Document the decision/s for Risk Treatment**
 - *Level of authority*

Risk Mitigation Methodology



Source: NIST SP800-30

Mitigate Risk

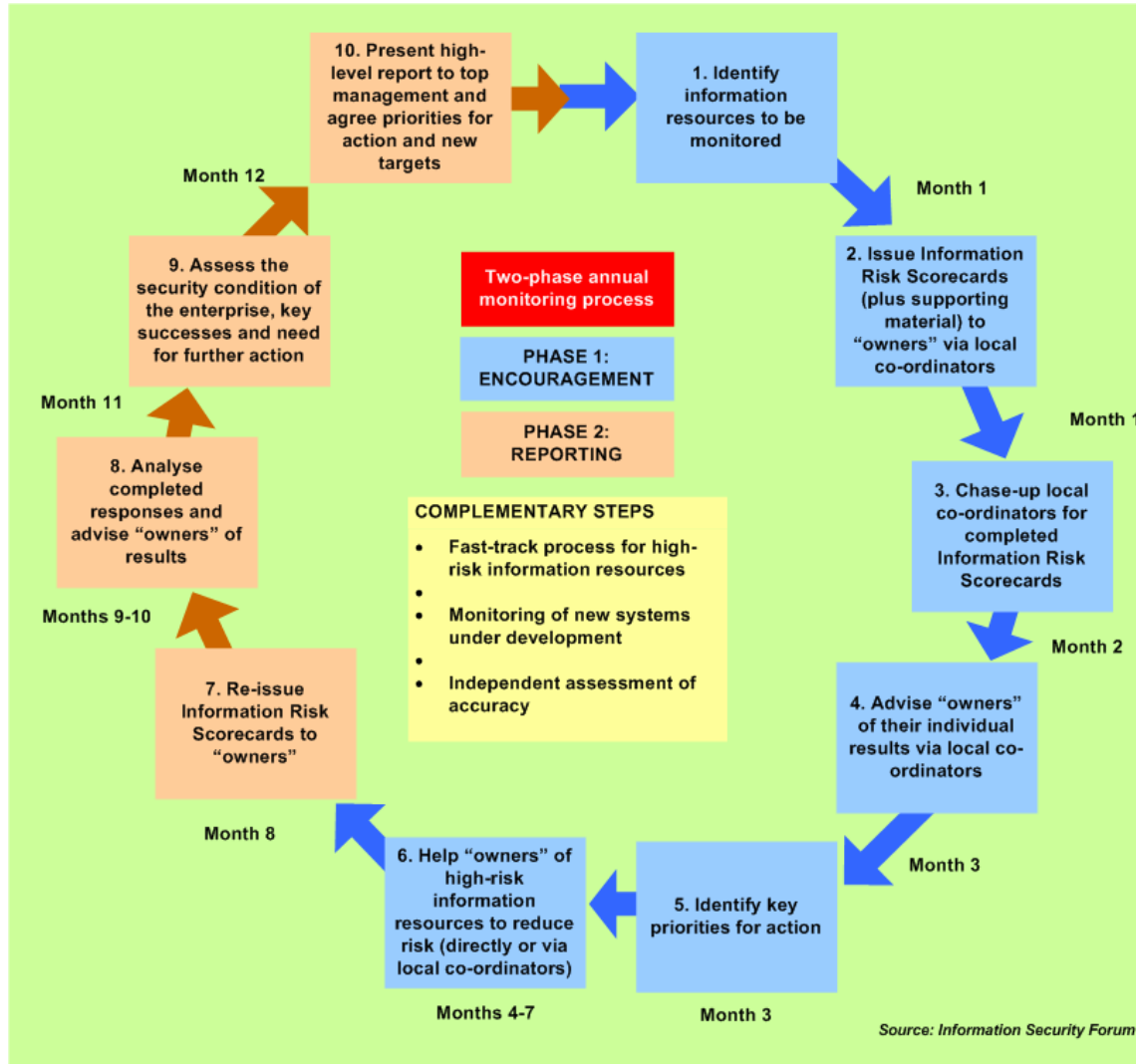
▪ **Implement Risk Controls**

- Document control design, configuration & maintenance
 - *Identify Key Risk Indicators (KRI's) for Monitoring*
- Plan the implementation (Change Management process)
 - *Acquire*
 - *Test*
 - *Back-out Plan*
 - *Communicate*
 - *Schedule*
 - *Implement*

▪ **Transition to Operations**

- Establish monitoring & reporting parameters

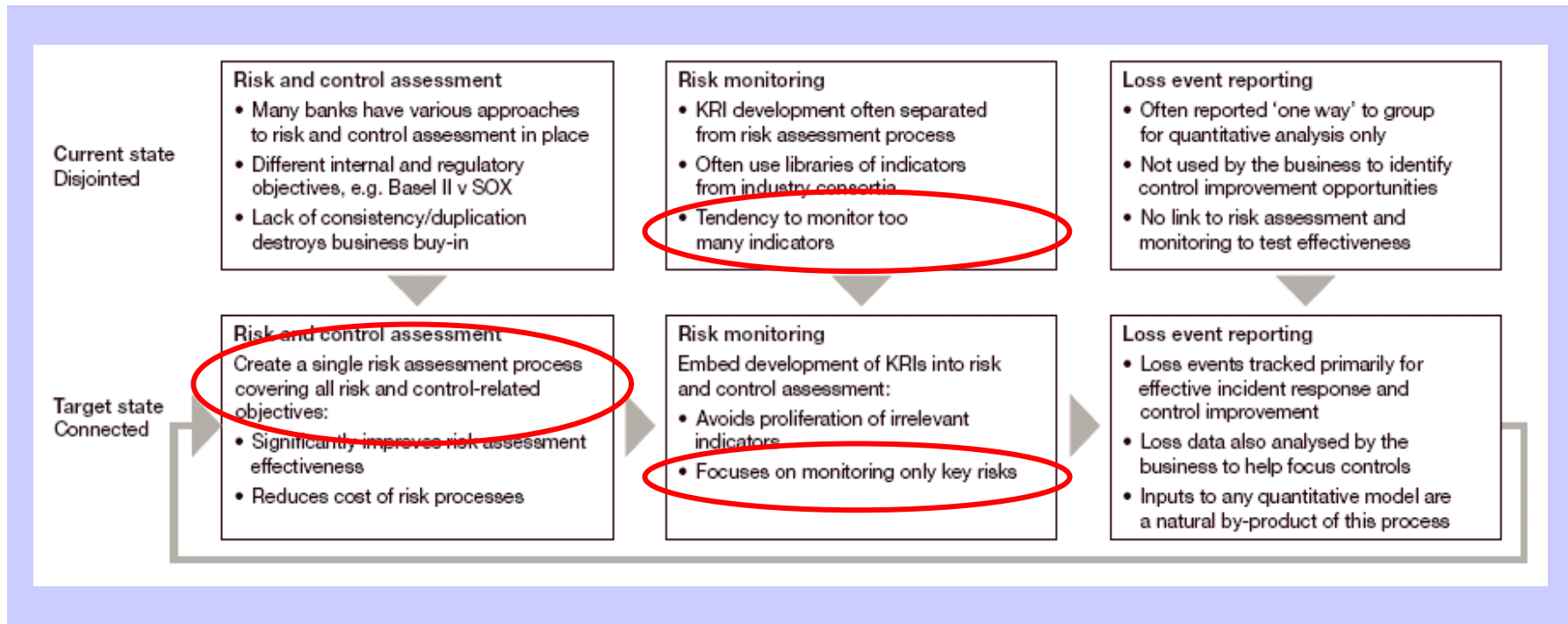
Monitor Risk



Mapping COBIT to IT-ORM

Traditional Risk Management Phase	COBIT
<ul style="list-style-type: none">▪ Risk Governance▪ Risk Analysis	Plan & Organize
Strategies for Risk Management /Treatment	Acquire & Implement
Implement Risk Mitigation Controls	Deliver & Support
Monitor	Monitor & Report

Suggested IT-ORM Improvement Process: Linking Operational Risk Management Processes



Source: *connectedthinking

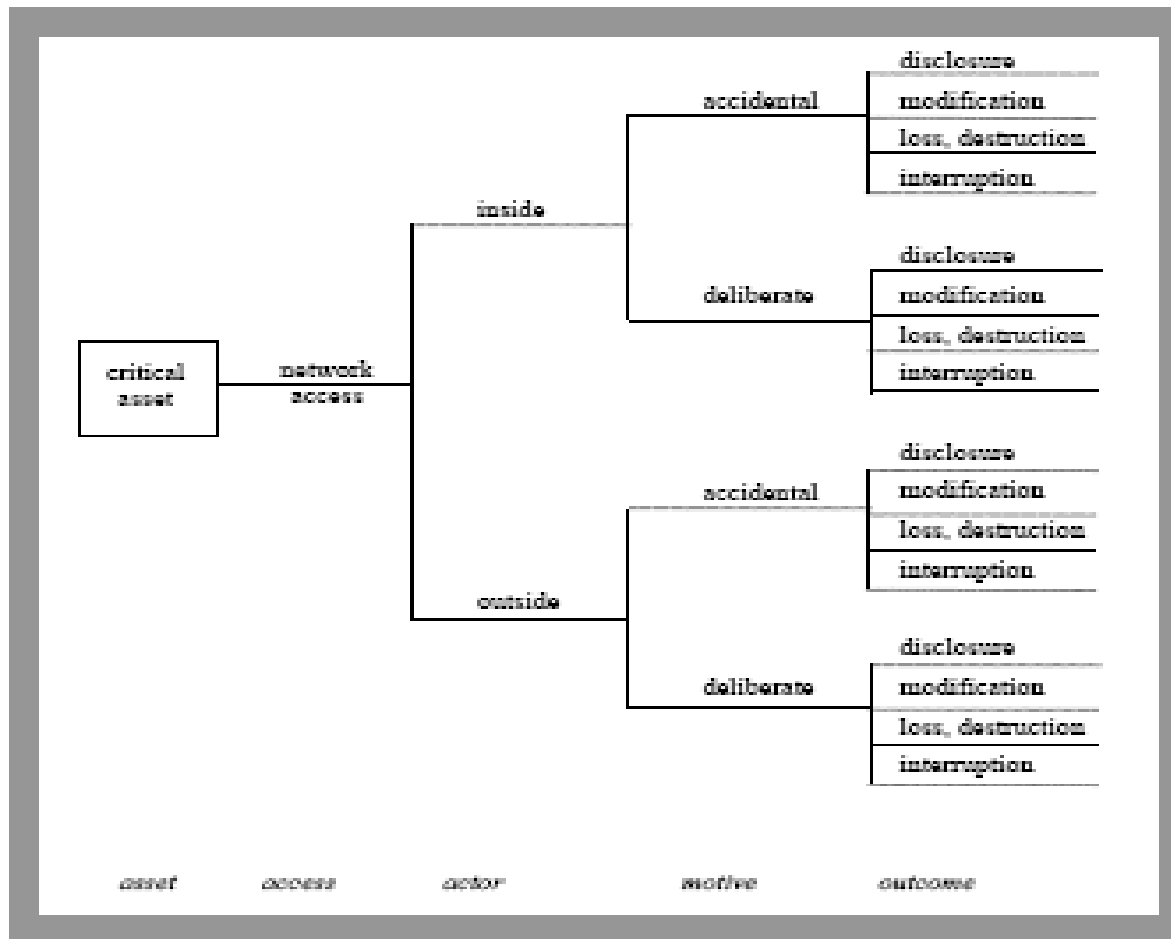
PRICEWATERHOUSECOOPERS PwC

Risk Management Methodologies

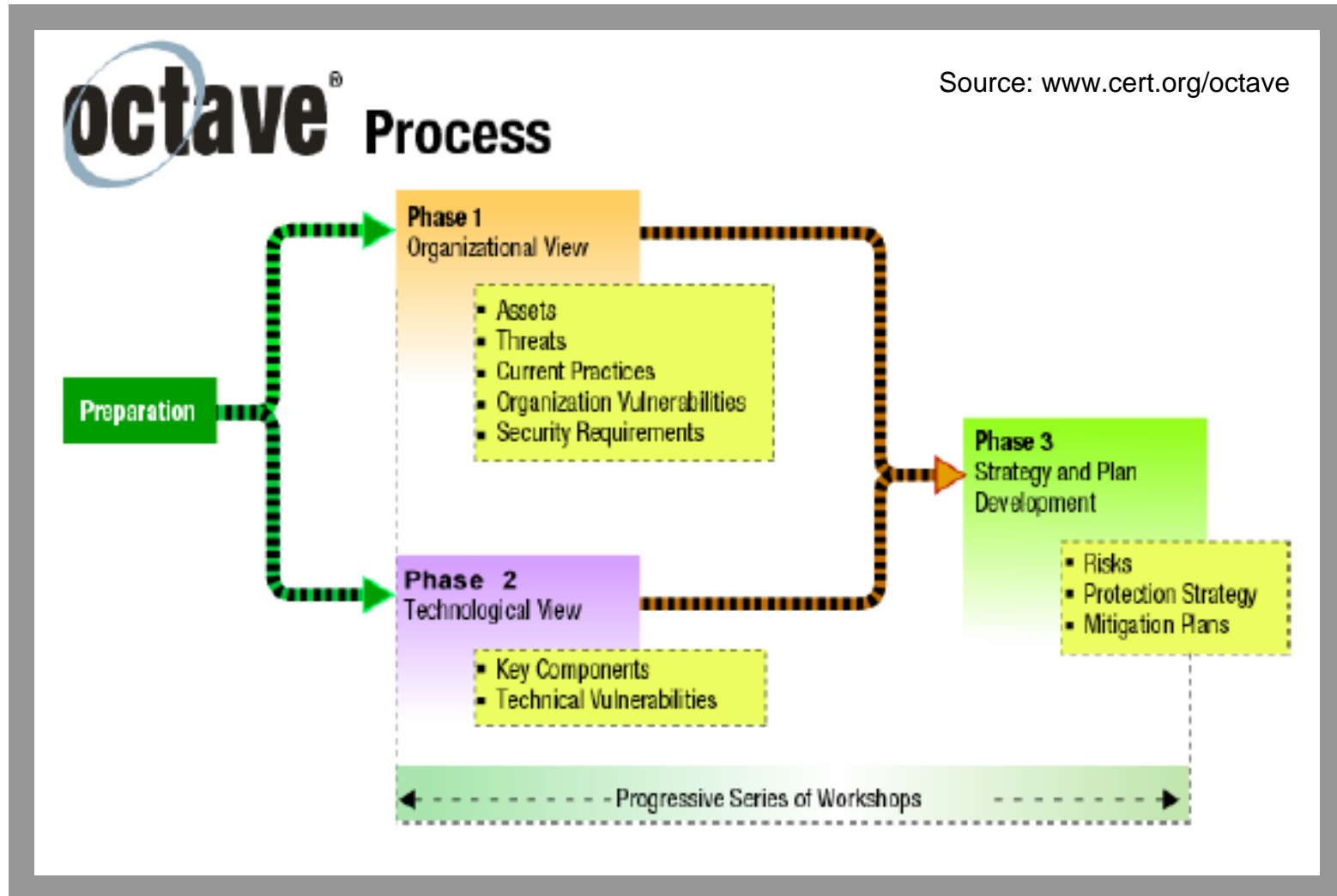
- ***National Institute of Standards & Technology, Special Publication SP 800-30***
 - Risk Assessment
 - Risk Mitigation
- ***Government of Canada – Communications Security Establishment TRA Working Guide (Document # ITSG04)***
 - Planning: Scope, Boundary, System Description, Target Risk & Required Certainty
 - TRA Preparation
 - *Statement of Sensitivity*
 - *Identification of System Assets*
 - TRA Analysis
 - *Identify Threat Scenarios*
 - *Filtering Threat Scenarios*
 - *Assessing Risk*
 - TRA Recommendations

Other Risk Management Methodologies: CM-SEI OCTAVE

- OCTAVE: Operationally Critical Threat, Asset and Vulnerability Assessment**



The OCTAVE Process



Benefits of IT Operational Risk Management

- **Knowledge of the threats, vulnerabilities & potential impacts (ignorance is NOT a valid excuse)**
- **Anticipating and minimizing potential financial impacts (costs to remediate, tangible & intangible losses)**
- **To minimize the exposure through suitable preventive measures**
- **Reduce the frequency & magnitude of incidents**
- **Detecting the events when they occur in a timely manner**
- **Being prepared to respond to the event, when it occurs**
- **Meet regulatory & compliance requirements**
- **Good corporate governance**

If we accept the premise that “something untoward will occur”, then there are obvious benefits to preparing for those events.

In other words, having the appropriate **PREVENTIVE** measures in place, being able to **DETECT** the events when they occur, and having the means to **RESPOND** in a timely, efficient and effective manner.

Key Messages for IT-ORM

- **Establish Risk Management Governance**
 - Obtain management commitment & support
 - Establish & Document Decision-making Process
 - Integrate into Enterprise Risk Management
- **Choose a recognized methodology**
 - Use Quantitative & Qualitative methods, as appropriate
- **Establish & Maintain Risk Register**
- **Establish meaningful measures (KRI)**
- **Monitor IT Risk on an on-going basis**

Last Words ...

***I keep six honest serving men
(They taught me all I knew);
Their names are What and Why and
When
And How and Where and Who.***

Rudyard Kipling

References

- **IBM Privacy & Security Services**

<http://www-935.ibm.com/services/us/index.wss/itservice/bcs/a1000405>

- **Information Systems Audit and Control Association (ISACA)**

<http://www.isaca.org>

- **IT Governance Institute (ITGI)**

<http://www.itgi.org>

- **National Institute of Standards and Technology (NIST)**

<http://csrc.nist.gov/>

- **National Security Agency Security Configuration Guides**

<http://www.nsa.gov/ia/index.cfm>

- **International Standards Organization**

<http://www.iso.org>

- **Information Security Foundation (ISF)**

<http://www.securityforum.org>

- **Carnegie Mellon University, Computer Emergency Response Team (CERT)**

<http://www.cert.org/>

Q&A

Thank You!



To learn more about **IBM Canada's Security & Privacy Services**, visit

www.ibm.com/ca