IT Risk Management: What a (Competent) Corporation Wants?

Slaven Smojver, PhD, CRISC, CISM, CISA
slaven.smojver@hnb.hr

December, 2021

The views expressed in this presentation do not necessarily reflect the views of the Croatian National Bank

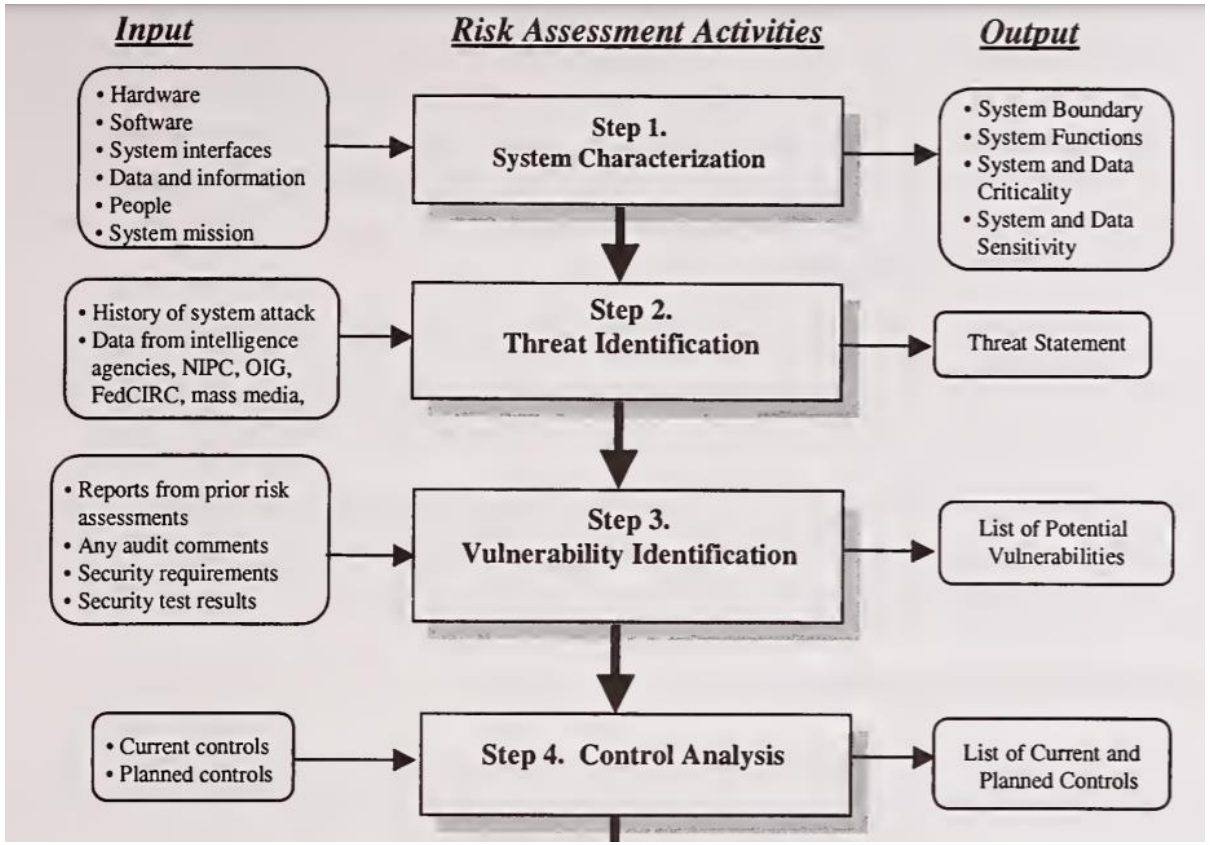
Brendan Fraser Alicia Silverstone

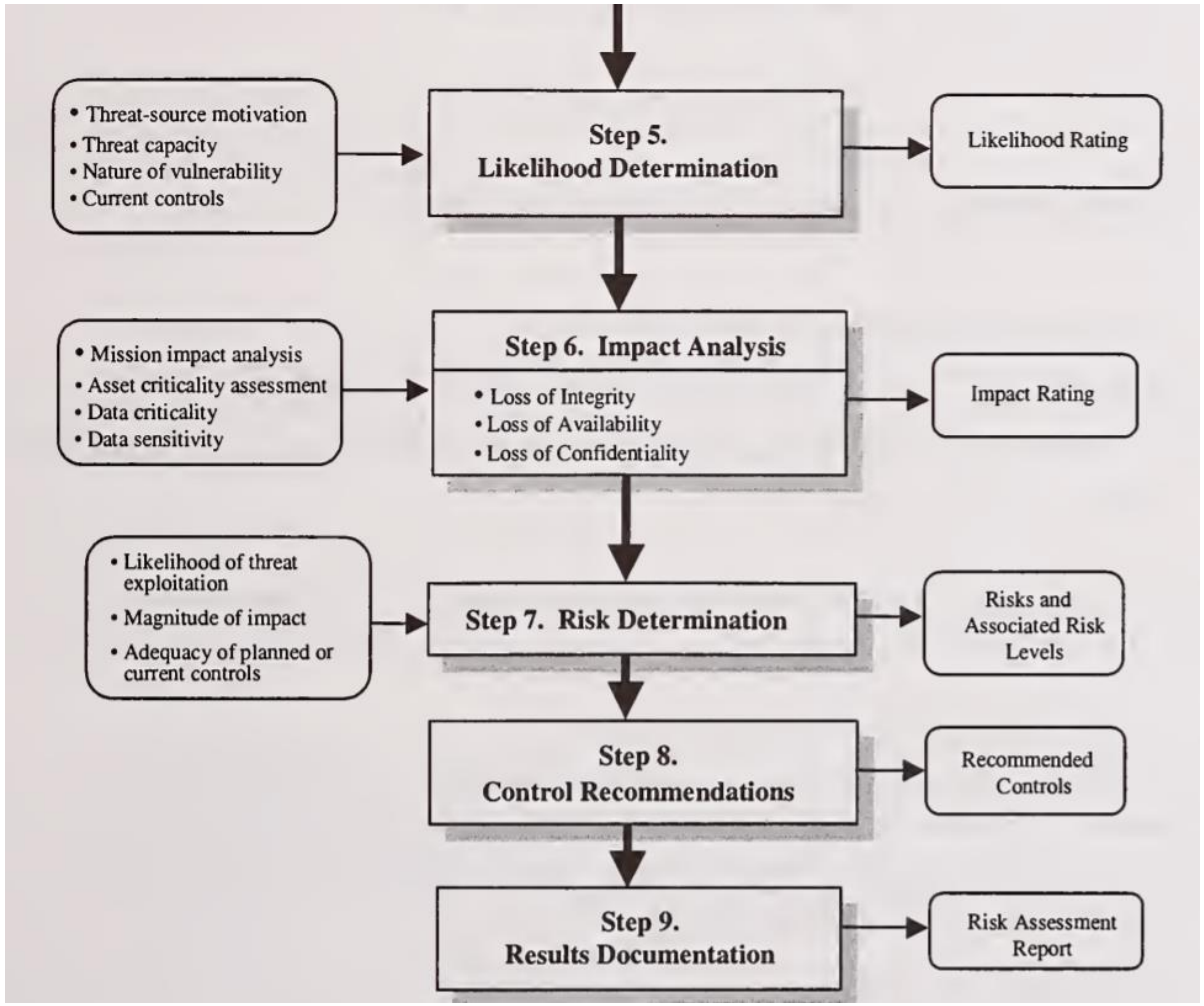
Blast From the Past

2002

NIST Special Publication 800-30

(Risk Management Guide for Information Technology Systems)





Source:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

2002

NIST Special Publication 800-30

(Risk Management Guide for Information Technology Systems)

Likelihood Level	Likelihood Definition
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.

Magnitude of Impact	Impact Definition
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.

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

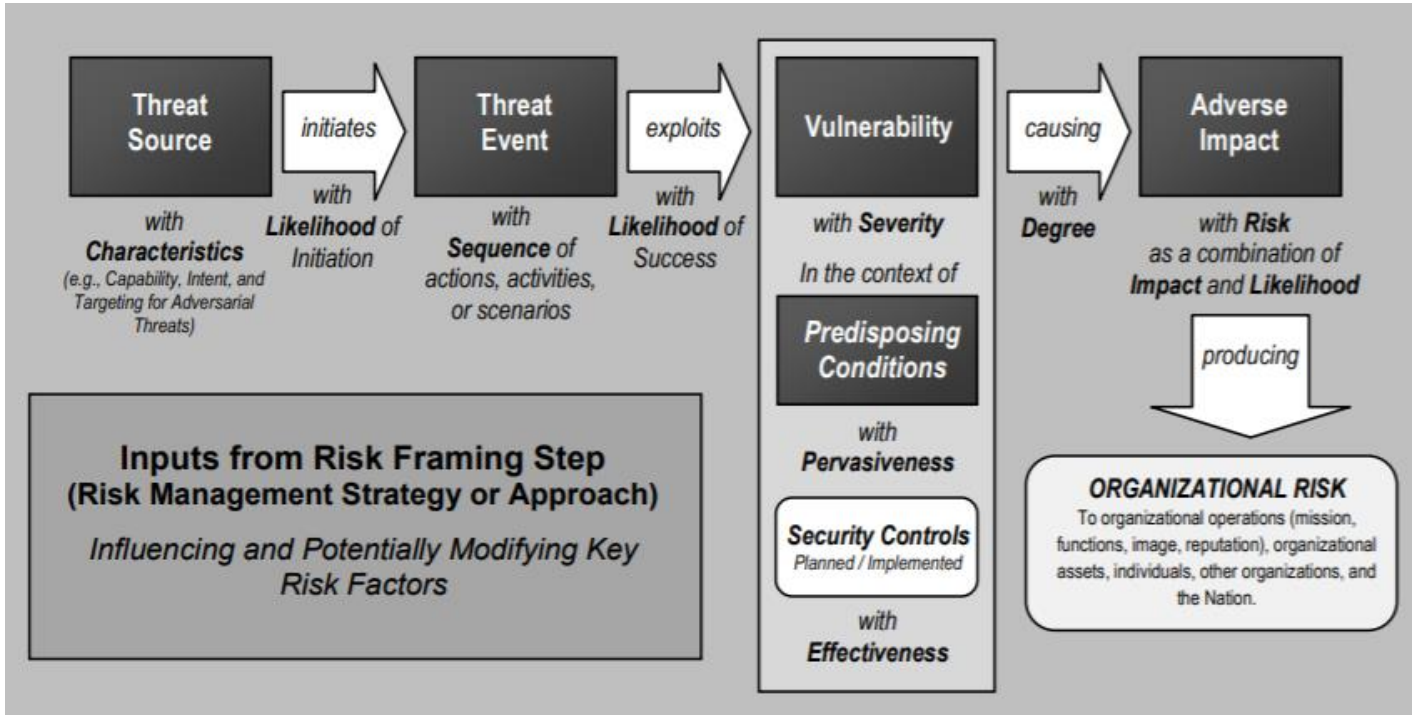
Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

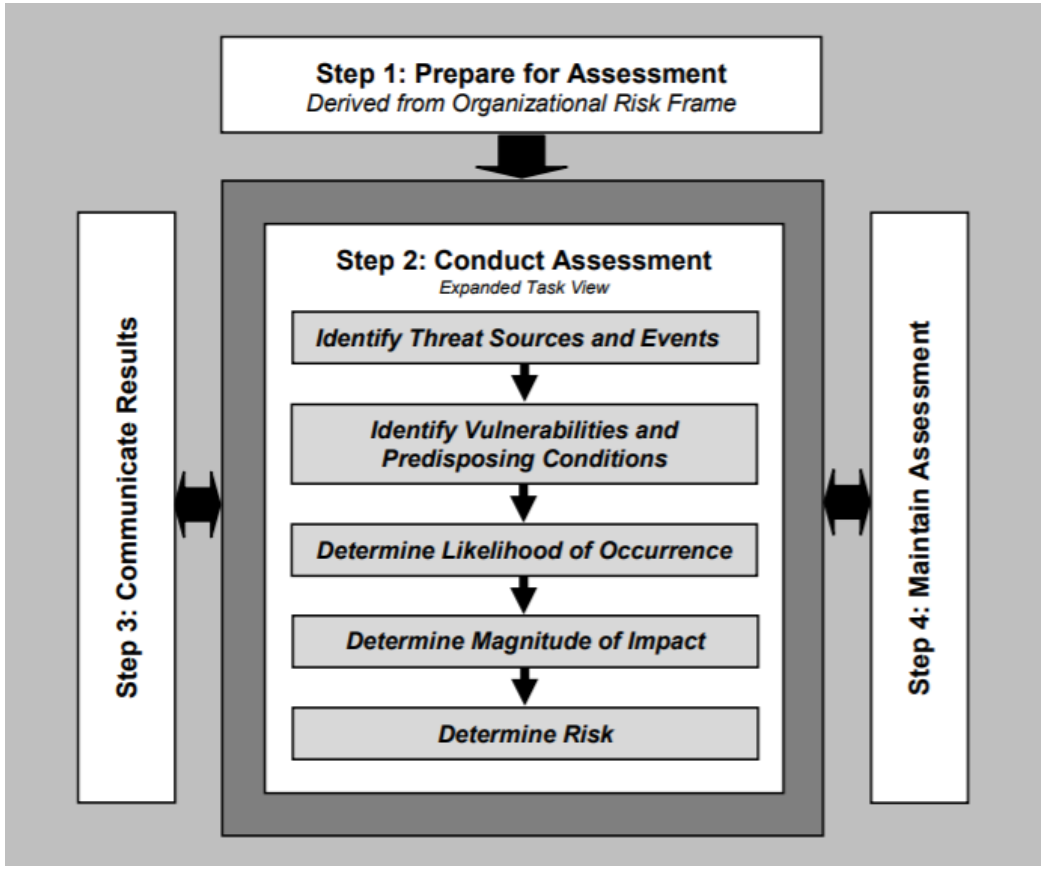
Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation 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.

2012

NIST Special Publication 800-30 rev. 1

(Risk Management Guide for Information Technology Systems)





Source:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

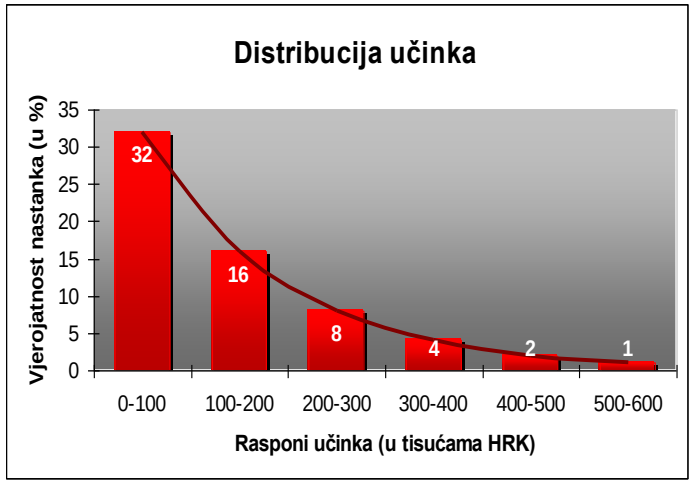
2006 - 2010

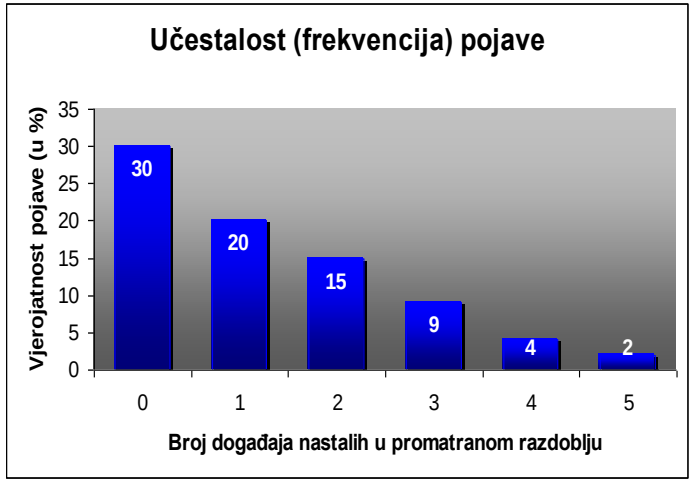
Basel II i modeliranje operativnog rizika

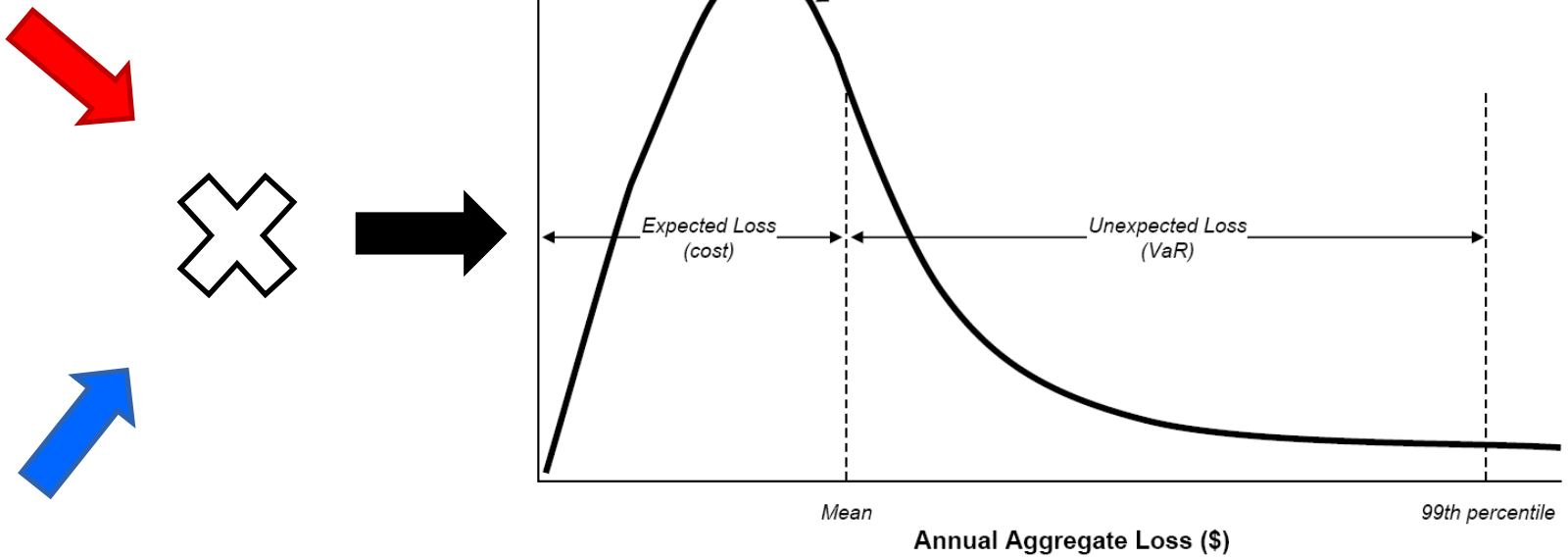
- Samad-Khan, 2005 i 2006:
  - Banka srednje veličine utvrdila je da bi joj za identificiranje i dokumentiranje rizika u svim procesima trebale 192 čovjek/godine.
  - „Fantomski rizici" - požar s katastrofalnim posljedicama po organizaciju koji se događa u prosjeku jednom tjedno ili krađa velikog iznosa koja u prosjeku nastaje svaki dan.
  - Vjerojatno je da će se organizacije usredotočiti na neželjene događaje koji su im poznati, a zanemariti će se mogućnost pojave neželjenih događaja za koje ne znaju.
- „Tradicionalne" metode rizik promatraju kao kombinaciju učinka i frekvencije (često kao umnožak) u većem broju "diskretnih" točaka → takve se kombinacije vjerojatnosti pojave događaja i učinka nazivaju rizikom.
- „Novi" pristupi upravljanju operativnim rizikom smatraju da bi trebalo promatrati cijeli spektar (odnosno kontinuitet) različitih učinaka i učestalosti pojave neželjenog događaja.
  - velik broj kombinacija daje kontinuiranu a ne diskretnu razdiobu.
  - distribucija učinka i distribucija učestalosti

2006 - 2010

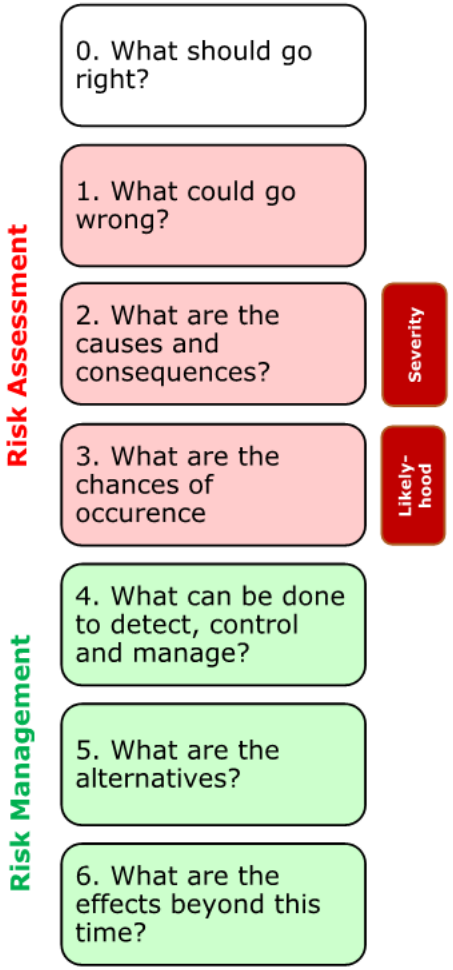
Basel II & modelling approaches to operational risk







Operational Risk Management



0. What should go right?

1. What could go wrong?

Negative scenario identification:
a. Using historical information
b. Using comparative analysis
c. Predefined lists of risks
d. Team-based elicitation
e. Modelling

2. What are the causes and consequences?

Causal chain of events → Identification of root causes

Cause-analysis tools

Fish-bone diagram Pareto chart Scatter diagram	Fault tree analysis (FTA) Cause-consequence analysis (CCA)

3. What are the chances of occurence?

4. What can be done to detect, control and manage?

Guiding questions:
1. Which segments can be detected? (earlier = better)
2. Which causal events can be controlled and how?
3. How can the system recover quickly?

5. What are the alternatives?

Risk treatment strategies: reduce chance of occurrence, reduce consequences or reduce both:
1. Detect and break causal chain
2. Control: separate or suppress
3. Recover: duplicate, disperse or transfer

6. What are the effects beyond this time?

Effects of risk treatment alternatives.

Risk Assessment Methods

1. **Preliminary Hazard Analysis (PHA)**
   Table-format assessment that contains ORM steps 1. – 4.

2. **Hazard & Operability Analysis (HAZOP)**
   Top-down qualitative reductionist approach for discovering (possible) deviations. Combines *guidewords* (not, more, less, high, low) with system parameters (temperature, speed, pressure,…).

3. **Failure Mode and Effect Analysis (FMEA)**
   Table-format assessment starting from ORM question 0. Useful for complex systems. Can be used for systems, sub-system or components.

4. **Fault Tree Analysis (FTA)**
   Top-down analysis of causes of failure (sketch of chain of events). Useful for complex systems. Can be used in comb. with PHA, HAZOP, FMEA

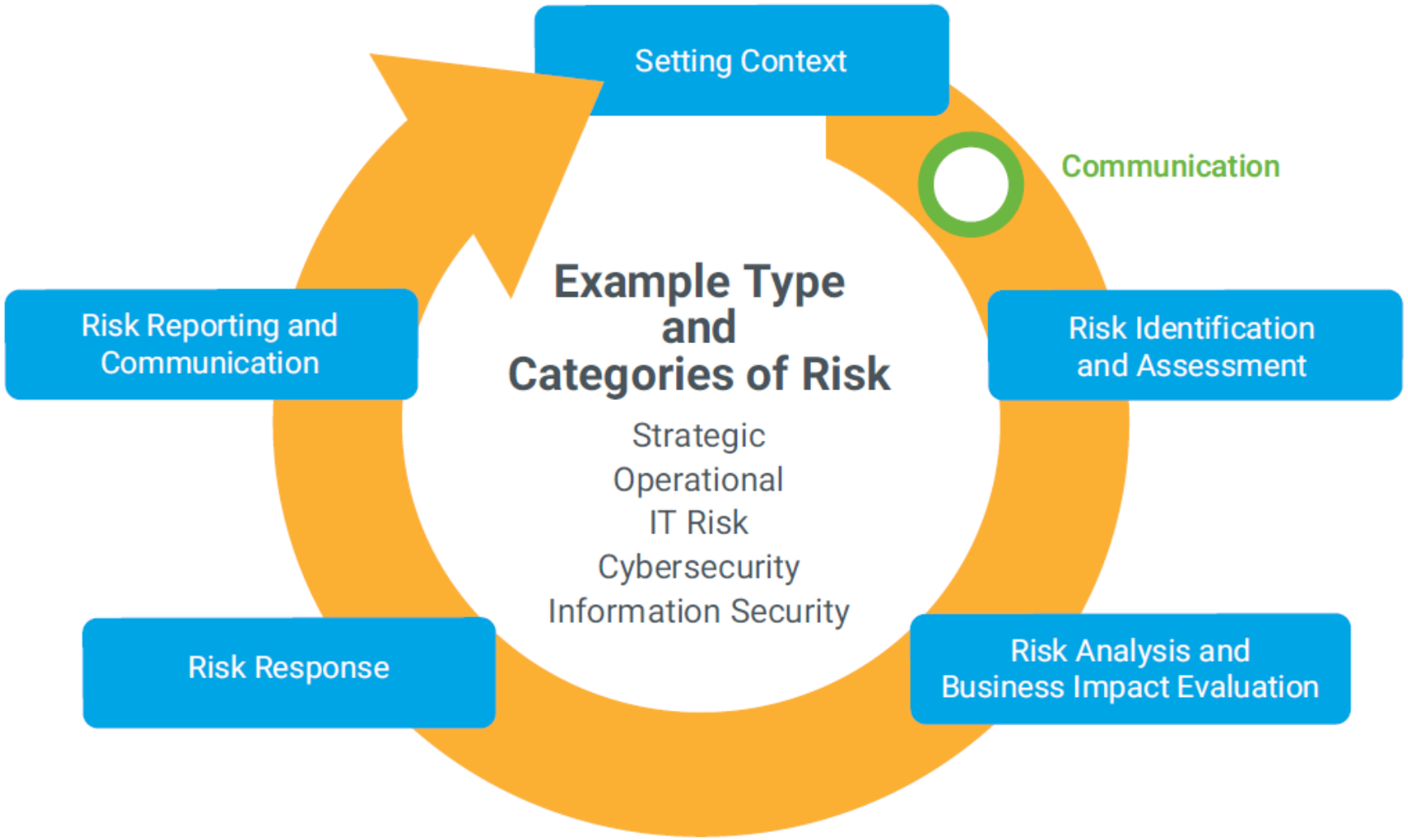
5. **Cause and Consequences Analysis (CCA)**
   Visual, chronological demonstration how failure happens and what are the consequences (*Bowtie* diagram). Can encompass FTA.

6. **Event Tree Analysis (ETA)**
   Event tree (possible consequences) with probabilities.

7. **As low as reasonably practicable (ALARP)**

ISACA Risk IT Framework

Risk Management Workflow

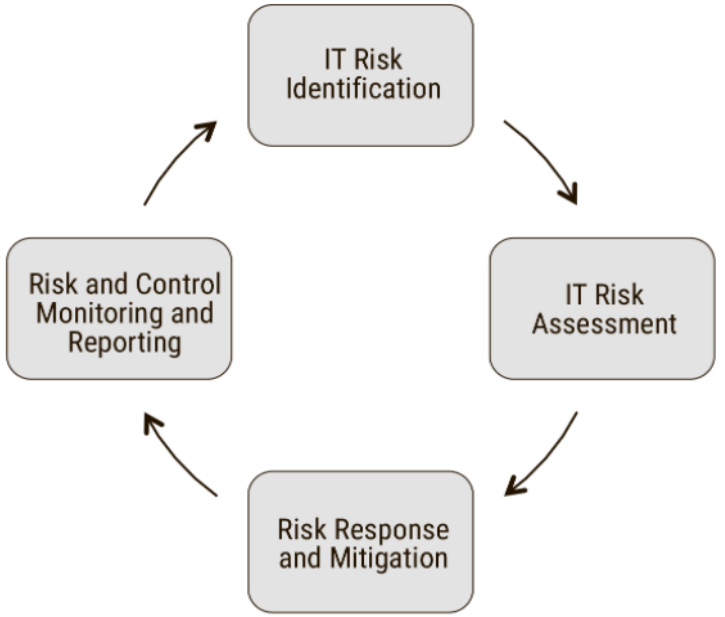


Source:
ISACA Risk IT Framework, 2nd edition

IT Risk Management Steps

- Risk identification (determine risk context, framework, appetite, tolerances & process for identifying & documenting risk; result = listing & documentation of threats to assets, controls efficacy, vulnerabilities and potential impact)
- Risk Assessment (analysis and evaluation of threats to assess and prioritize risks in relation/context to organization's risk appetite and criteria for deviations where risk tolerances will be increased)
- Risk response and mitigation (cost-effective ways to address the identified and assessed risk)
- Risk and control monitoring and reporting (controls, RM efforts and current risk state are monitored and reported to SM)

Figure 1.5—The IT Risk Management Life Cycle



IT risk = business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within enterprise.

Source:
CRISC Review Manual 2021

Three Lines of Defence (3LoD) and Risk Practitioner

- **1st line – operational management**. Provision of products and services to clients and managing risk. Business unit that performs daily operation activities – implement policies (business owners = risk owners). They implement RM policies and have to implement and monitor implemented controls. Responsible for implementing corrective actions (for risks above the appetite) and for implemented controls to keep risk within tolerable levels.
- **2nd line – risk and compliance**. Expertise, support, monitoring and challenge on risk-related matters. Establish RM frameworks, monitor and ensure that businesses operate in accordance with the ERM policies, standards & procedures. Monitor & report on enterprise current risk profile, posture, exposure, status of risk mitigation and significant & credible threats faced by the organization. 2nd line continuously interacts with the 1st line and is therefore somewhat subjective to it. Their important task is gaining enterprise-wide consensus, buy-in and adoption of the ERM framework.
- **3rd line – audit**. Gaining appropriate level of assurance to the SM and the board through independent and objective review. Auditor should assess conformance of the RM program to the selected standard, review and evaluate design and implementation of the RM and ensure efficacy of the 1st and 2nd lines.

RP often works across 1st and 2nd line. RP is uniquely positioned to act as advisory on variety of risks and threats that the org. is facing, analysis and assessment of risk, selection of appropriate risk response and reporting on changes to the enterprise's risk posture, profile and overall exposure.

Role of the Risk Practitioner (RP)

- Focus on risk not from only one department perspective. To understand goals and objectives of the enterprise → active dialogue and regular communication SM ←→ RP. RP should (through communication) validate the understanding of vision & strategy and how they translate to technology and business units (some things might be confidential).
- Executives will (at the end) choose path which offers the best prospects for value creation. RP should not be obstructionist to that process (cannot always say no!) by ensuring that they:
  - Understand the business in proper context
  - Listen & understand strategy
  - Build relationships in organization (so that RM processes are embedded in business processes & new projects)
  - Create culture to encourage open communication
  - Advise on risk, but do not make decisions for the business.

Risk → considers potential losses and opportunities.

Organizational Structures, Roles and Responsibilities

Figure 1.8—Sample RACI Chart

Task	Senior Management	Steering Committee (Chair)	Department Managers	Risk Practitioner
Collect risk data	I	A	C	R
Deliver the risk report	I	A	I	R
Prioritize risk response	A	I	R	C
Monitor risk	I	A	R	C

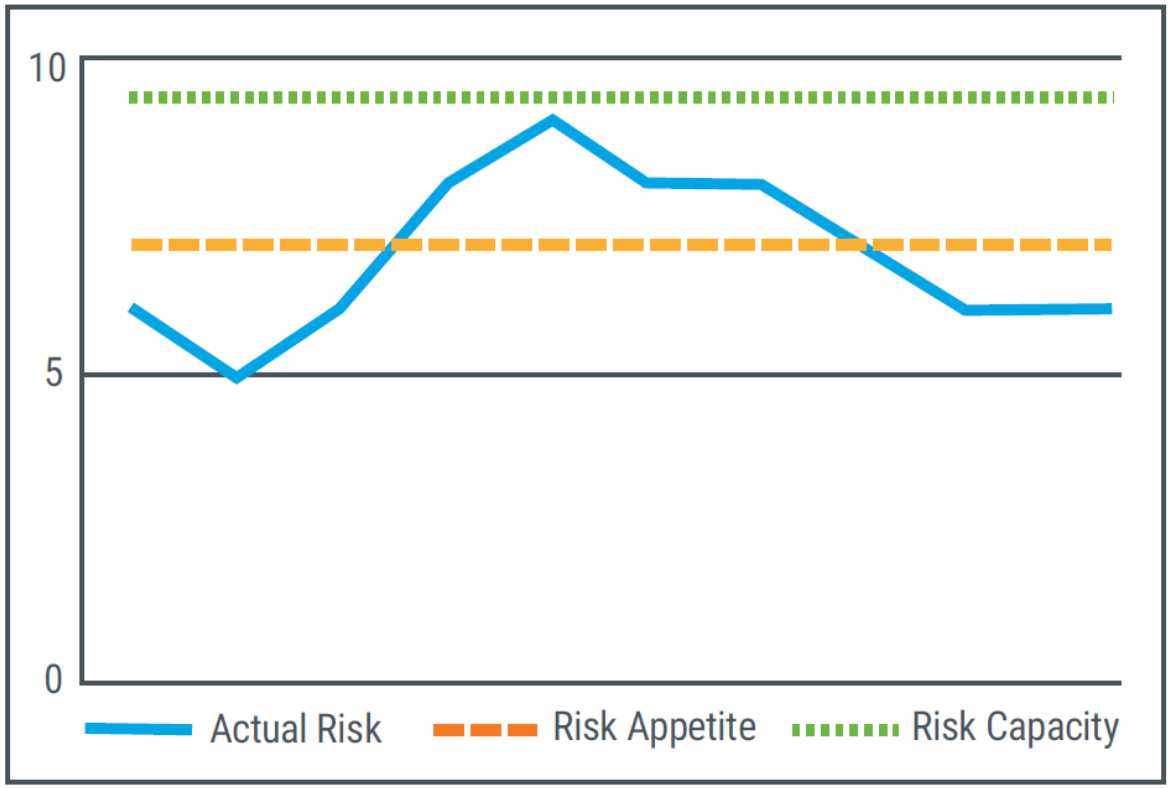
Source:
CRISC Review Manual 2021

Key roles in RM:

- Risk manager (RM) = responsible to ensure that RM functions are carried out to support organization's goals and objectives.
- Risk analyst = responsible for analysis, evaluation and assessment
- Risk owner = accountable for making risk-based decisions (owns the loss realized by the scenario).
- Control owner = accountable for ensuring controls are designed, implemented and operating as planned to keep risk at acceptable level (could be risk owner).
- Control stewards = responsible for management and maintenance of controls (on behalf of the risk owner).
- Subject matter experts are those that have relevant knowledge (usually consulted).

Risk Capacity, Risk Appetite and Actual Risk

- **Risk capacity** = objective amount of loss an enterprise can accept without its continued existence being questioned.
- **Risk appetite** = amount of risk (on a broad level) that org. is willing to accept in pursuit of its mission. Determined by the risk owners and BoD (may be delegated to SM).
- **Risk tolerance** = Deviations from risk appetite (permissible, if predefined criteria is fulfilled).



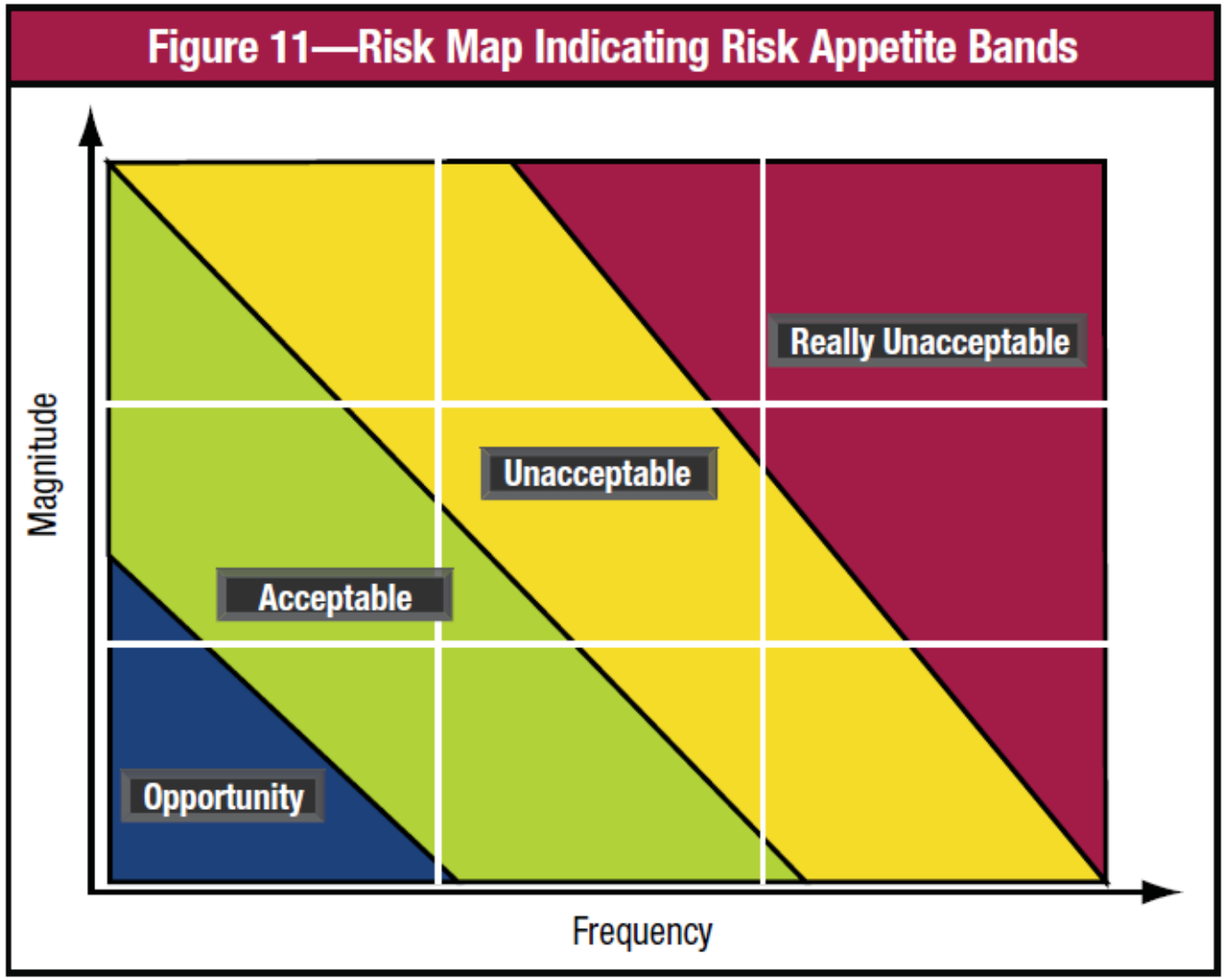
Risk acceptance should not exceed appetite and must not exceed capacity.

Source:
ISACA Risk IT Framework, 2nd edition

Risk Appetite and Risk Culture

- Determining risk appetite (RA) **of** senior management is a significant challenge for RP. It may differ across different business lines, it may change over time... → requires periodic review.
- **Risk culture**:
  - Set of beliefs and shared values that governs attitudes towards risk taking.
  - Willingness to embrace, cautiously accept or avoid risk.
  - Set by the SM.
  - Best indicator of the risk culture = how decisions on how to respond to various risks are made.
- Risk culture elements:
  - Behaviour towards risk-taking (risk averse vs. risk-taking); how much risk can be absorbed, and what is it willing to take? Problem if stated policy is very different from observed behaviour.
  - Behaviour towards negative outcomes (learning and adapting vs. blame & no root-cause); how to deal with losses, missed opportunities, etc.?
  - Behaviour towards policy compliance (compliance vs. non-compliance).

Risk Appetite and Risk Mapping



Source:
ISACA Risk IT Practitioner Guide, 2009

Development of Risk Scenarios

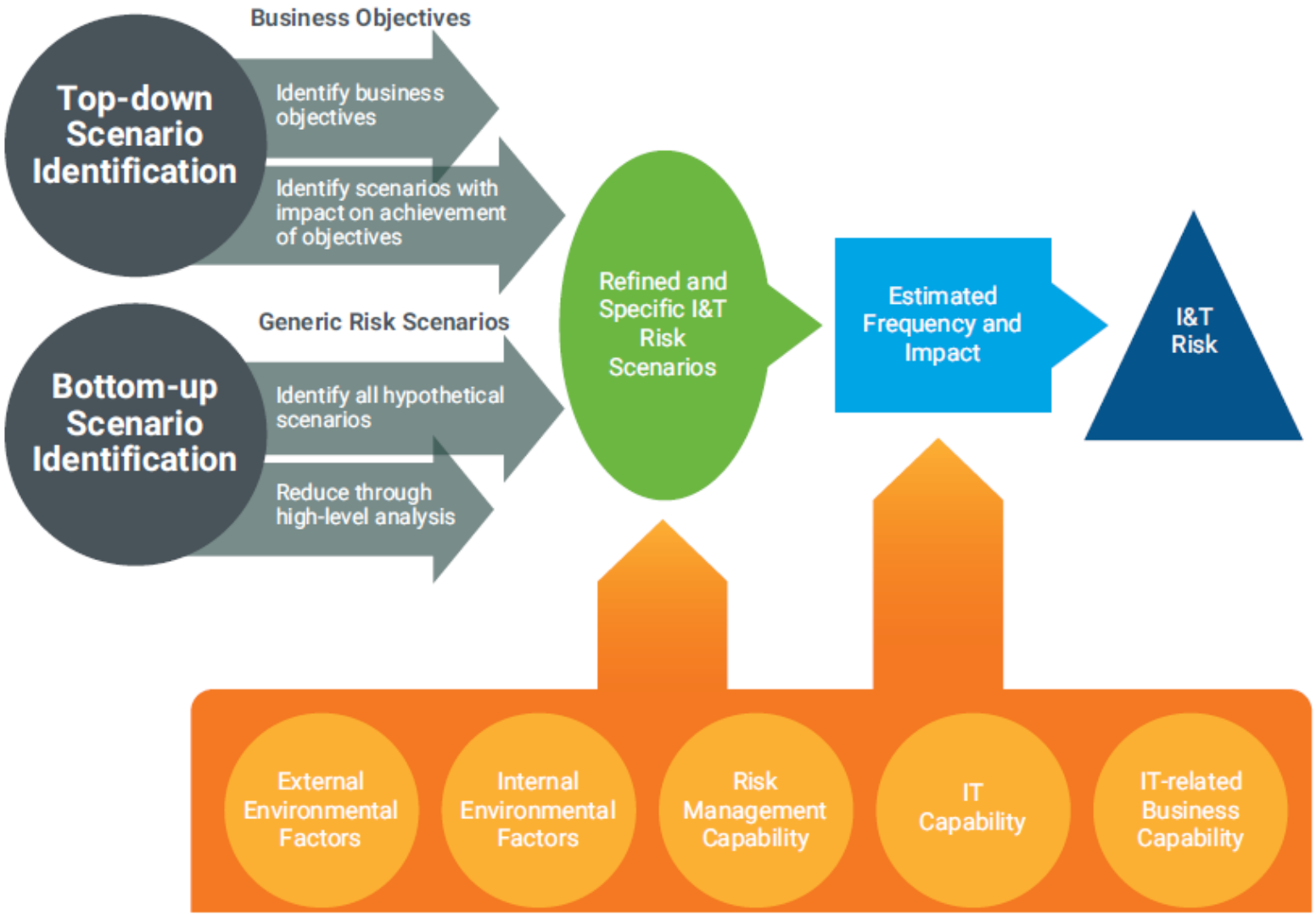
Risk Scenario = a description of a possible threat event whose occurrence will have an uncertain (negative or positive) impact on the achievement of enterprise's objectives that provides a way of conceptualizing risks. Used to document risk in relation to business objectives or operations affected by the risk → useful as a basis for quantitative risk assessment.

Development of risk scenarios:

- Top-down. Understanding business goals & how they could be affected by risk events and developing of various scenarios that are impacting those goals. A general approach that looks at IT and non-IT related events and is easier to understand by SM (even if they are not interested in IT).
- Bottom-up. Describing risk events specific to the org. RP and the team start with a more generic scenario and then hone it by adding details and complexity to account for coinciding events. Good method to identify scenarios that are particularly relevant for the org, but difficult for maintaining management's interest (because scenarios are highly detailed and technical).

Benefits of Using Risk Scenarios – gathering and framing info used in subsequent steps of RM. Construction of narrative that can inspire people to act. Helping RM team to explain risks to business owners and other stakeholders. Provides a realistic & practical view of risk.

Development of Risk Scenarios



Source:
ISACA Risk IT Framework, 2nd edition

Generic IT Risk Scenarios

Figure 40—Generic IT Risk Scenarios *(cont.)*

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk	Risk Consequence		Risk	Risk Consequence	
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
11	Software implementation	Internal	Failure	Ineffective execution	Process (enable operation and use) Enterprise architecture (applications)	Timing (non-critical) Duration (moderate) Detection (instant)		P		• Operational glitches when new software is made operational • Users not prepared to use and exploit new application software					
12	IT project termination	Internal	Failure	Ineffective execution	Process (retire the programme)	Timing (critical) Duration (extended) Detection (Slow)		P		• Failing (due to cost, delays, scope creep, changed business priorities) projects not terminated			• Failing or irrelevant projects stopped on a timely basis		
13	IT project economics	Internal	Failure	Ineffective execution	Process (monitor and report on the programme)	Timing (non-critical) Duration (extended) Detection (slow)		P		• Isolated IT project budget overrun • Consistent and important IT projects budget overruns • Absence of view on portfolio and project economics			• IT project completed within agreed-upon budgets		

Source:
ISACA Risk IT Practitioner Guide, 2009

Issues Related to Risk Scenarios

- Currency of risk factors and scenarios. Solution: develop a review schedule (at least annually or when changes occur).
- Generic scenarios as starting point, then add detail. Group scenarios and start from generic to keep the number of scenarios manageable. Assumptions made when grouping should be understandable and well documented.
- Nr. of scenarios ≈ business reality and complexity. RM is about reducing (not increasing!) complexity. However, retained scenarios need to accurately reflect business reality and complexity.
- Adequate people and skills for scenario development, including:
  - Expertise and experience to not overlook relevant and ignore highly unrealistic or irrelevant. Although highly infrequent but catastrophic should be considered.
  - Understanding of environment (IT, business and their interaction).
  - Alignment of involved parties
  - Developing scenarios via brainstorming/workshop and reducing number of scenarios to manageable but relevant & representative number.

Issues Related to Risk Scenarios

- Risk taxonomy should reflect business reality and complexity.
- Use generic risk scenario structure to simplify risk reporting (not detailed for each sub-scenario).
- Use scenario building for buy-in from involved parties. Gaining buy-in is the reason for careful facilitation.
- Involve 1st line into scenario building (including some of the staff that knows details).
- Do not focus only on rare & extreme scenarios (worst-case).
- Deduce complex scenarios from simple, by cascading and/or coincidental impacts (e.g. major hardware failure + DRP failure, DB corruption + failed backups, etc.).
- Consider systemic and contagious risk.
- Use scenario building to increase awareness for risk detection – what if the org. doesn’t know that it doesn't know about the risk event? Detectability relies on visibility and recognition.

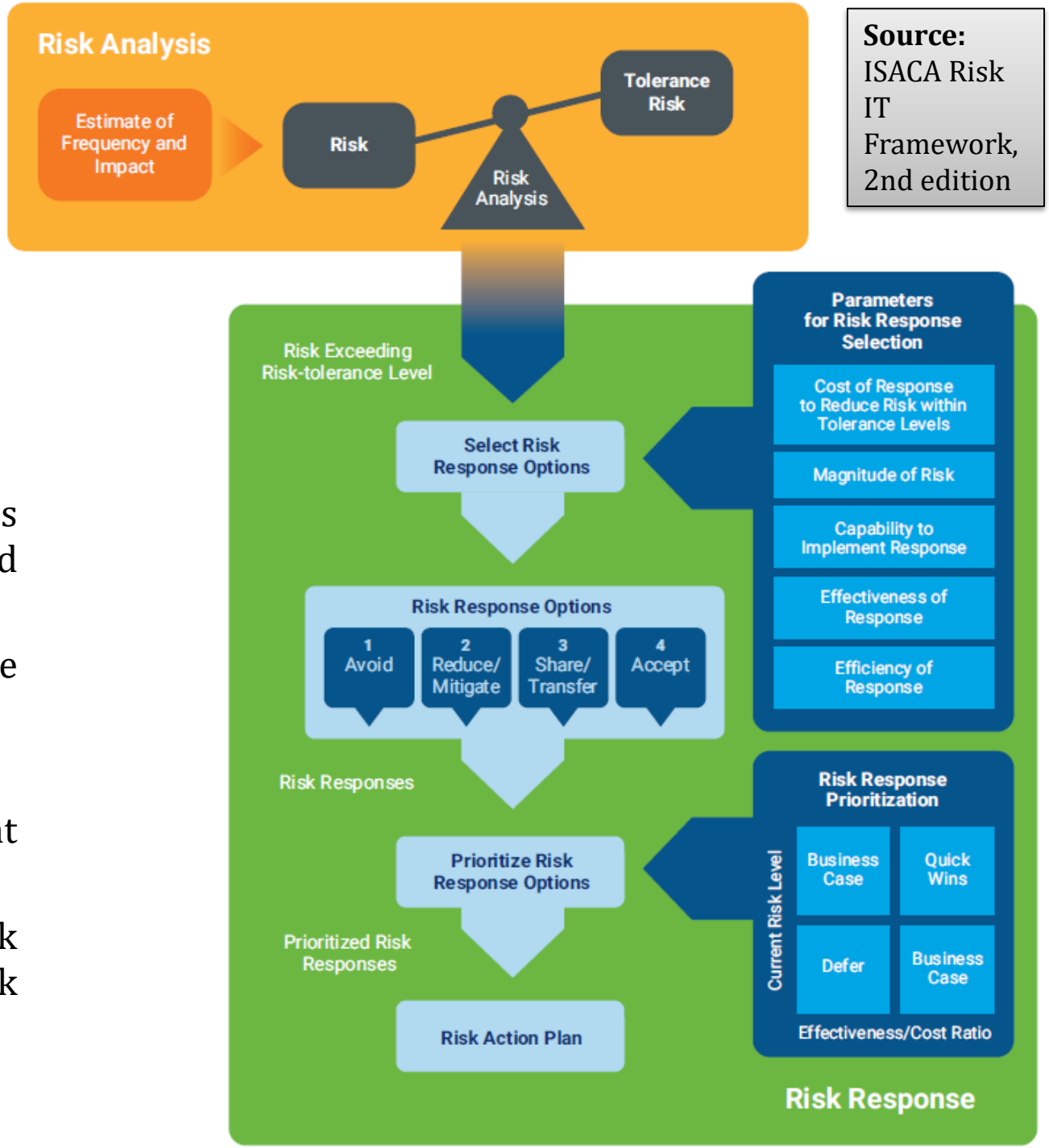
What Should Risk Practitioner do After Risk Assessment?

- **Risk Ranking** = RP uses results of the risk assessment to place risks in an order that can direct the risk response effort.
- **Risk Maps**. After the risk has been determined, RP need s to review whether risk levels are within boundaries of acceptable risk, as determined by the SM. Based on the position of a certain scenario on the risk map, RP can make assessment on what could be appropriate risk response.
- **Documenting Risk Assessments**. At the end, RP creates comprehensive report for the SM.

Risk register consolidates risk data into one place and enables tracking. It is one document with all detected risks (containing severity, source, impact, owner, current status, etc.) and should document the entire risk universe of the org. It should be current and periodically reviewed. It can be accompanied by a controls register.

Risk Response Selection and Prioritization

1. Risk scenarios drive risk analysis and assessment.
2. Risk analysis leads to mapping of risks.
3. Risk response is determined by the management's risk appetite (risk within appetite should be accepted and beyond appetite should be treated).
4. Risk response options are examined to determine the best available response.
5. Selected response is documented.
6. Risk responses are prioritized according to current environment & cost-benefit.
7. Risk treatment plan is created to manage risk response project (reviewed and approved by the risk owner and added to the risk register).



Source: ISACA Risk IT Framework, 2nd edition

Choosing a Risk Response

- Factors that management may consider while deciding what is the best risk response:
  - Risk priority (in risk assessment report).
  - Complexity of recommended controls.
  - Cost of response (acquisition, impact on productivity, training, maintenance, licensing)
  - Management decision (considering financial objectives, risk tolerance and appetite, relative importance, etc.).
  - Compliance requirements.
  - Alignment of response with org's strategy.
  - Organizational culture.
  - Time, resources and budget.
  - Environmental and market conditions.
- The primary criteria → value obtained for a given cost. Inherently a management decision, but RP is involved in framing the question and in answering.

Risk responses should be documented in risk register with clear accountability and timeframe for implementation. Plan of action and milestones (POA&M) documents actions that have yet to be done (controls often cannot be implemented instantly). RP should ensure that POA&M are periodically reviewed are plans for controls are not abandoned.

Risk Practitioner and Risk Response

- RP should communicate current and expected risk responses with the owner.
- Risk owners (RO) should actively drive RM activities performed by RP to ensure desired outcomes. There should be a direct link between risk and control: Risk justifies control and control is traceable to risk. RO is accountable for ensuring that control's effectiveness is monitored.
- RP may conduct risk/benefit analysis for alternative responses to risk (in business case) or calculate ROI.
- RP should evaluate effectiveness of each control and verify the correct balance between administrative, technical and physical controls.
- RP has a key role in ensuring that controls are properly set up, operated, maintained, with results regularly reported to management.
- RP should ensure that mitigation project has been implemented according to design and that changes did not diminish effectiveness.

RP should not decide on behalf of the organization, his role is to ensure that management has the best information to make the decision.

RP has a key role in ensuring that controls are properly set up, operated, maintained, with results regularly reported to management.

Risk Monitoring and Reporting

- RP should remember that purpose of the control is to mitigate risk → purpose of monitoring should not be whether control is working, but whether it effectively addresses risk. RP should continuously monitor, benchmark and improve IT control environment & control framework to meet organizational objectives. When monitoring shows noncompliance or ineffectiveness, RP should recommend mitigation activities (new or adjustment of controls; change in business process).

- RPs are commonly expected to report to management and BoD on the status of RM & overall risk profile of the org (requires review of effectiveness of controls and their compliance with established policy).

KPIs, KRIs & KCIs

- Performance indicators measure how well a process is performing in terms of it stated goal. KPIs = subset of PIs.
- Risk indicators are used to measure risk levels in comparison to certain thresholds, so that org is alerted when risk level approaches unacceptable level (org. can respond before unacceptable outcomes). KRIs are a subset of RIs that are highly relevant & poses a high probability of predicting or indicating important risks.
- Control indicators show the effectiveness of controls. KCIs are a subset of CIs that quantify how well a specific control is working. Goal of KCIs: track performance of control actions relative to tolerances → ongoing insight into adequacy of a given control in keeping risk within acceptable levels.

Thank you for your attention!

Questions, comments…