Univerza v Mariboru
Fakulteta za logistiko

UPRAVLJANJE IT TVEGANJ S POMOČJO Risk IT

Doc. dr. Borut Jereb
Doc. dr. Boštjan Brumen

Izziv

- Tveganje je sestavni del poslovanja.
- Potrebno ga je učinkovito upravljati.
- Upravljanje IT tveganj je največkrat odrinjeno v domeno tehničnih specialistov.
- Tehnični specialisti niso vključeni v odločanje, zato je IT tveganje na poslovnem nivoju največkrat prezrto.

Risk IT kot odgovor na izziv

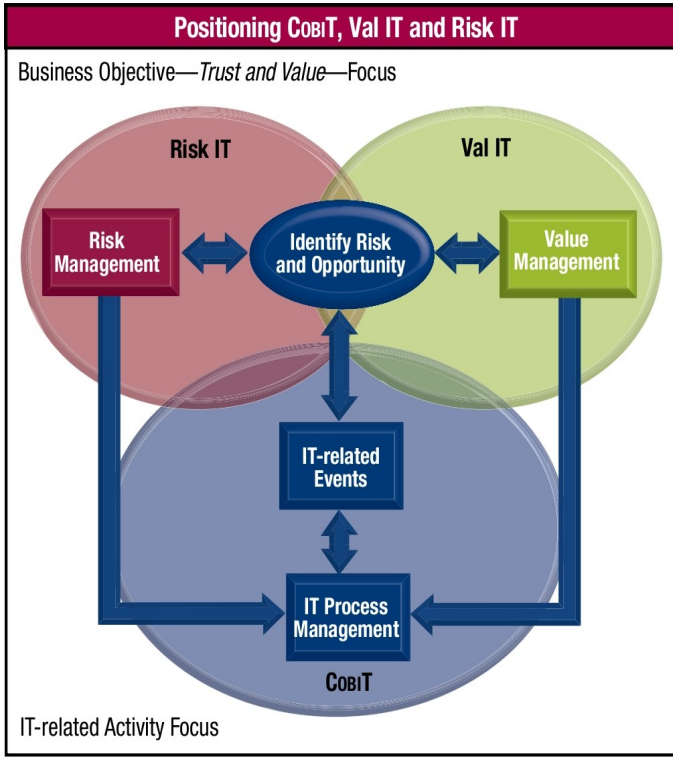
- Predpostavka: IT tveganja so del poslovnih tveganj (kot strateška, tržna, kreditna, etc) in ne zgolj operativnih tveganj.
- Vključujejo odgovornost posameznikov vpletenih v aktivnosti upravljanja.
- Navodila okvira *Risk IT* komplementarno dopolnjujeta okvira COBIT in Val IT.
- Navodila so učinkovita tudi v primeru samostojne uporabe.

Lastnosti *Risk IT*

- Dobrodošel odgovor na zahteve posameznikov in podjetij/organizacij po orodju za upravljanje IT tveganj.
- Bolj splošen (in verjetno bolj uporaben) kot ISO/IEC 27005:2008.
- Ne definira natančno kaj tveganje sploh je.
- Ne definira orodij za samo zaznavanje in ocenjevanje tveganj.

Ozadje

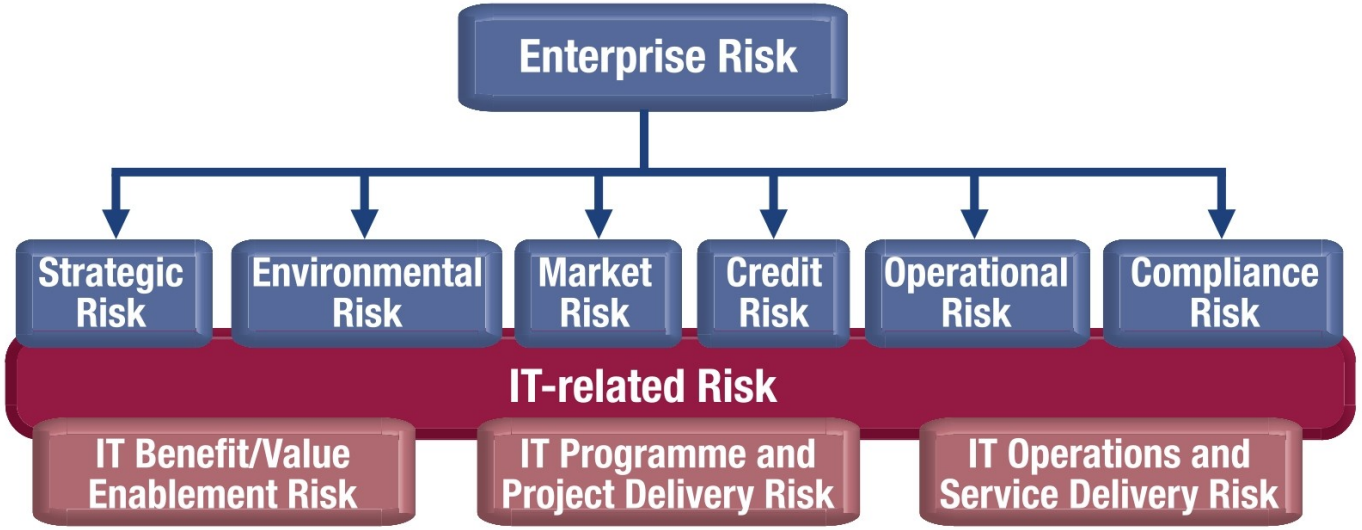
- ISACA: Kontrolni cilji za informacijsko in sorodno tehnologijo – **COBIT**.
- ISACA: Upravljanje investicij v IT – **Val IT**.
- ISACA: Upravljanje tveganj v IT – **Risk IT**.
- Medsebojno komplement.
- V zadnjem času še:
  - ISO/IEC 27005:2008 in
  - ISO/IEC 31000:2009



Kategorije IT tveganj

- Kategorije IT tveganj so povezana z:
  - doseganjem poslovnih vrednosti, ki jih IT nudi,
  - projekti in investicijskimi programi in
  - obratovanjem in vzdrževanjem IT.

Figure 3—IT Risk in the Risk Hierarchy



Lastnosti IT tveganj

- IT na mnogih področjih poslovanja prinaša koristi in tveganja.
- Zaradi pomembnosti IT je potrebno IT tveganja obravnavati kot poslovna tveganja.
- IT tveganje ni zgolj tehnično vprašanje.

Deležniki pri upravljanju IT tveganj

- Deležniki upravljanja IT tveganja so: uprava podjetja, vodja upravljanja financ, vodja upravljanja tveganj, regulatorji na nivoju države ali ceha, zavarovalničarji, vodja IT, vodje poslovnih področij in drugi.

Principi - 1

- Pri upravljanju IT tveganj moramo zagotavljati:
  - Stalno upoštevanje poslovnih ciljev organizacije.
  - Usklajenosti upravljanja IT z ostalimi tveganji.
  - Uravnoteženosti med stroški in koristmi.
  - Odprto komunikacijo o IT tveganjih.
  - Osebne odgovornost posameznikov (odnosi in odgovornosti dobro definirane; jasne meje tolerance.
  - Neprekinjeno, vsakodnevno opravilo, ki ga moramo po potrebi izboljševati

Principi - 2


Risk IT Principles
Connect to Business Objectives
Align IT Risk Management With ERM
Balance Cost/Benefit of IT Risk
Promote Fair and Open Communication
Establish Tone at the Top and Accountability
Function as Part of Daily Activities
Risk IT Principles

Procesi -1

- Za upravljanje tveganj, Risk IT predvideva:
  - devet procesov upravljanja tveganj
  - združenih v tri skupine:
    - upravljanje tveganj,
    - vrednotenje tveganja in
    - odziv na tveganje.

Procesi -2

Figure 6—Risk IT Framework

Odgovornosti -1

- Za
  - vsak proces in za
  - vsako vlogo so
- predpisane
  - odgovornosti za izvajanje procesa (zagotovitev, da se aktivnosti v okviru procesa uspešno zaključijo) in
  - zahteve za sodelovanje v procesu (lastnik vira, ki je izpostavljen tveganju, potrjuje uspešnost izvajanja aktivnosti).

Odgovornosti - 2

Responsibilities and Accountability for IT Risk Management

Role Definitions		Risk Governance			Risk Evaluation			Risk Response		
Role	**Suggested Definition**	Common Risk View	Integrate With ERM	Risk-aware Decisions	Collect Data	Analyse Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Board	The most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources	●	●							
Chief executive officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise	○	○						●	
Chief risk officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	○	○	○	●	○	○	●	○	○
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	○	○	○	○	○	○	○	○	○
CFO	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks	○								
Enterprise risk committee	The executives who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.	○		○		○		○		
Business management	Business individuals with roles relating to managing a programme(s)	○	○	●		●	●	○	○	○
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	○	○	○	○	○	○	○	○	●
Risk control functions	The functions in the enterprise responsible for managing certain risk focus areas (e.g., chief information security officer, business continuity plan/disaster recovery, supply chain, project management office)	○	○	○	○	○	○	○	○	○
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise	○								
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit	○								○

Legend of the table:
- ○ Blue cell—The role carries responsibility and/or partial accountability for the process.
- ● Red cell—The role carries main accountability for this process. Only one role can be the main one accountable for a given process.

Kultura -1

- Upravljanje tveganj je odvisno od kulture (odnosa) do tveganj v neki organizaciji. Ločimo:
  - Sprejemanje tveganja: izogibanje in proaktivne ali celo agresivne.
  - Sprejemanje predpisov: kultura sprejemanja predpisov in zakonodaje običajna – njihovo delovanje je skladno s predpisi in zakonodajo delovanje, ki ni skladno s predpisi in zakonodajo.
  - Sprejemanje negativnih rezultatov (izguba, zgrešene priložnosti ali drugi negativni rezultati): zmožnost organizacije raziskati korenine problema tako, da se jim lahko naslednjič izogne.

Kultura -2

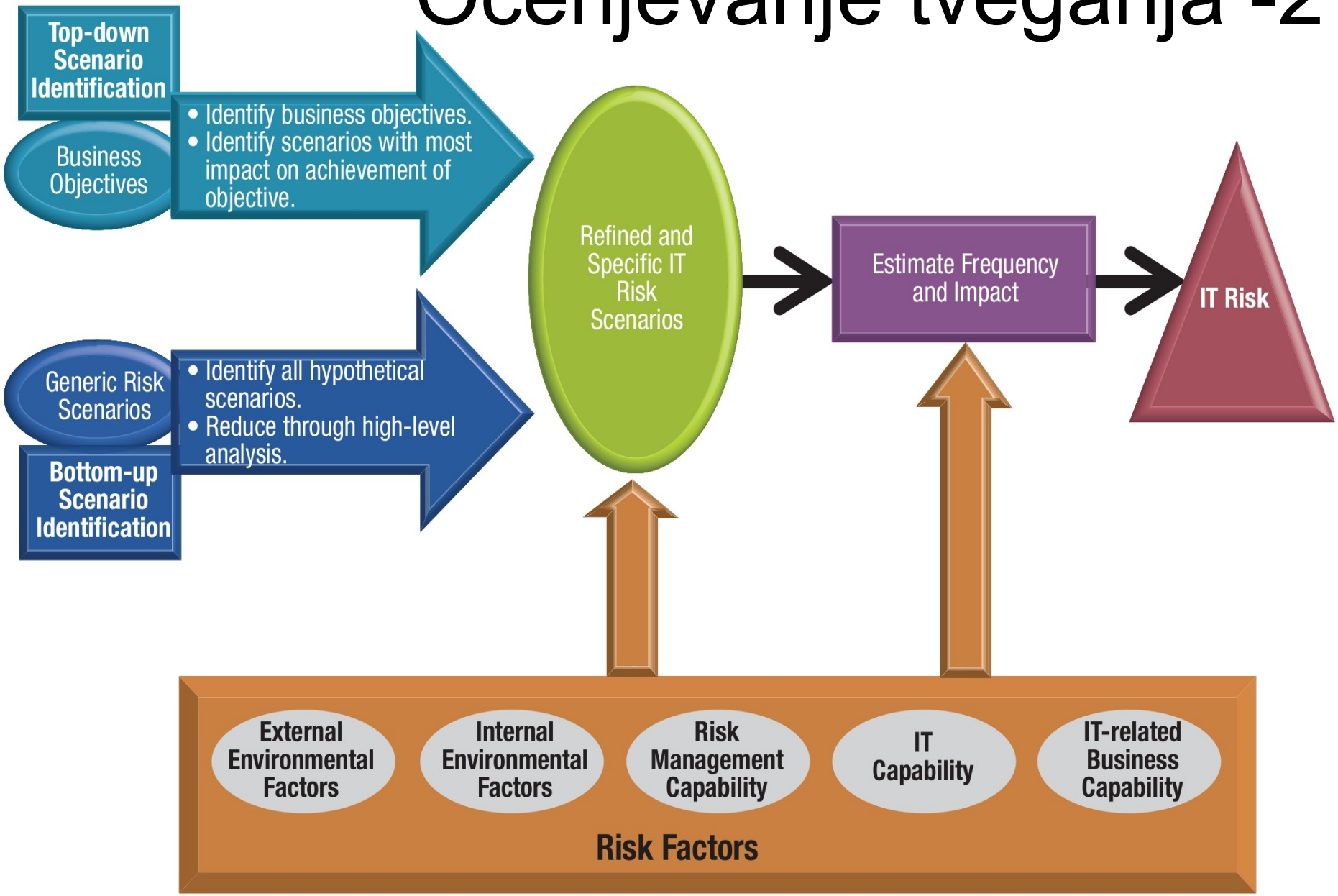

Elements of Risk Culture
Conservative: Risk-averse
Aggressive: Risk Taking
Behaviour Towards Taking Risk
Risk Culture
Learning Culture
Behaviour Towards Negative Outcomes
Blaming Culture
Behaviour Towards Policy Compliance
Compliance
Non-compliance

Ocenjevanje tveganja -1

- Določanje tveganj in njihovih atributov je verjetno najpomembnejše opravilo.
- Problem definicije tveganja.
- Problem statistike.
- Problem tveganj, ki se jih ne zavedamo in/ali jih ne poznamo.
- Pristop od zgoraj navzdol (poslovni vidik) in od spodaj navzgor (tehnični vidik).
- Faktorji okolja (zunanji vs. notranji).

Figure 13—IT Risk Scenario Development

Ocenjevanje tveganja -2



Odziv: Določanje indikatorjev tveganja

- Določimo ključne indikatorje tveganja:
  - Vpliv na poslovanje
  - Potrebna vlaganja za implementacijo, merjenje in poročanje
  - Zanesljivost predvidevanja
  - Občutljivost za predstavitev tveganja in variacije pojavnosti

Odziv: Prametri odločitve kaj napraviti s tveganjem

- Parametri odločitve:
  - Cena izbranega odziva.
  - Pomembnost tveganja.
  - Sposobnost za implementacijo odziva.
  - Uspešnost odziva.
  - Učinkovitost odziva (koristi odziva).

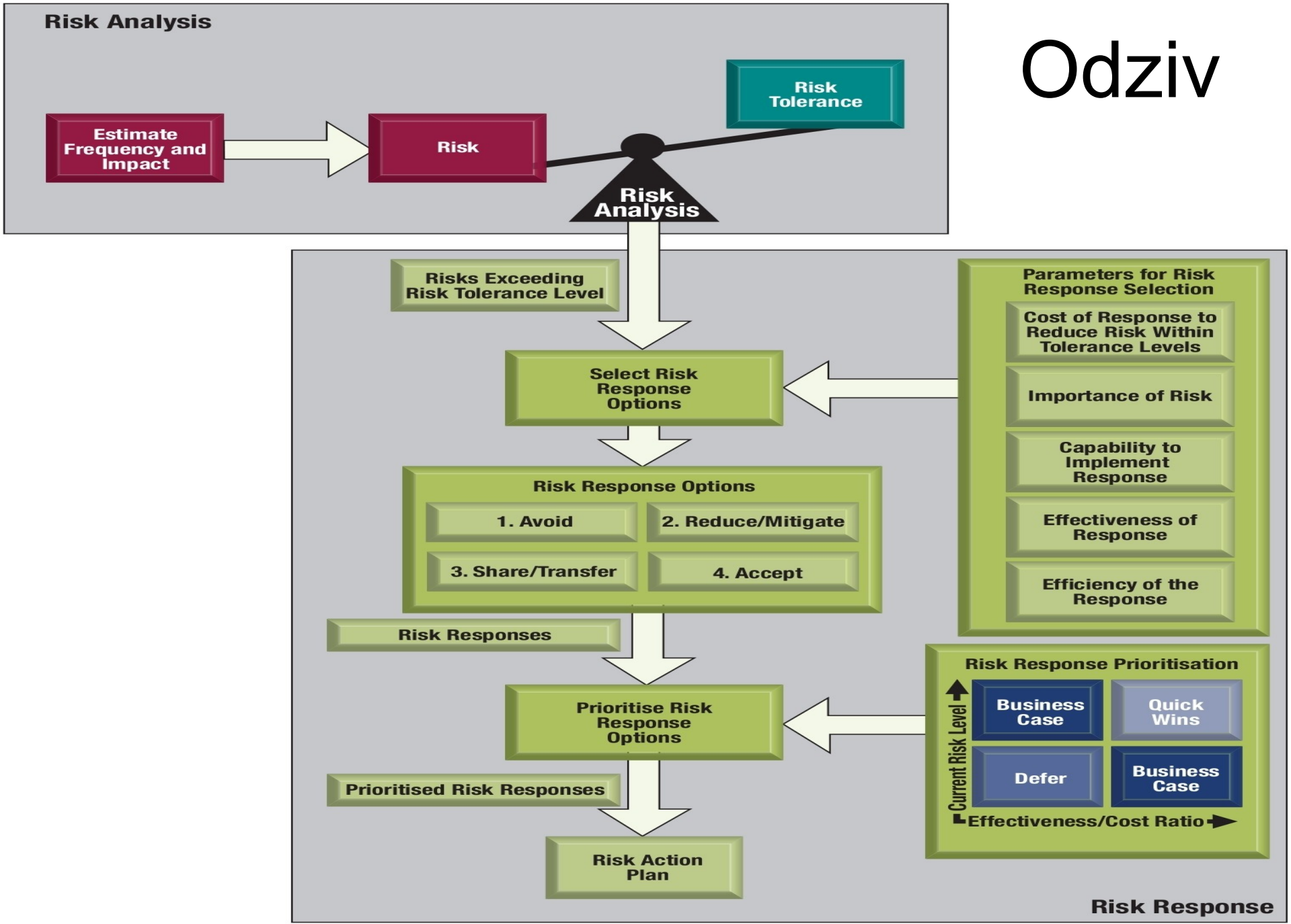
Odziv: Odločitev kaj napraviti s tveganjem

- Na osnovi poznanih indikatorjev se odločimo kaj napravimo s tveganjem:
  - Zmanjšamo
  - Sprejmemo
  - Se izognemo
  - Prenesemo na drugega

Odziv: Prioritete

- Na koncu določimo prioritete:
  - Hiter, močan odziv (visoka tveganja, velika predvidena škoda).
  - Izdelava poslovnega primera s pazljivo analizo višine vlaganj glede na tveganje in uspešnost odziva.
  - Odložen odziv ob nizkih tveganjih.

Figure 15—Risk IT Response Options and Prioritisation



Odziv

Zaključek

- *Risk IT* pokriva IT tveganja, ki so *povezana* z IT ob upoštevanju vseh tveganj.
- Dopolnjuje COBIT in Val IT.
- Predpostavlja, da so tveganja in koristi „dve strani istega kovanca“.
- Problem zaznavanja in definiranja tveganj ostaja odprt.
- Verjetno najpopolnejši in najuporabnejši dokument s področja upravljanja tveganj.

Vir vseh slik je:

The Risk IT Framework (2009); ISACA. ISBN 978-1-60420-111-6

Vprašanja

borut.jereb@fl.uni-mb.si