

New ICT & Security risk management framework

Mgr. Marek Zeman, PhD. CISO

Standards for managing risk in organization

Final Guidelines on ICT and Security Risk Managemnt (EBA/GL/2019/04)

- ☐ FMA Guide on ICT Security in Credit Institutions
- ☐ EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- ☐ PSD II / EBA PSD II Guidelines (2018)
- ☐ NIS-Guideline (EU) 2016/1148
- ☐ ISO/IEC 31000:2018
- ☐ ISO/IEC 27005:2018

- ☐ 18/2018 Z. z. zákon o ochrane osobných údajov
- ☐ 69/2018 Z. z. zákon o kybernetickej bezpečnosti

New EBA Guideline

The new EBA Guideline on ICT and security risk management (EBA/GL/2019/04) published on the 28th of November 2019

Basic requirements:

Risk category

- ICT & Security risk should provide a unified view of the following areas:
 - IT Availability and continuity
 - Security
 - Data Integrity
 - IT Outsourcing
 - IT Change management

Definition of SLOD

- Clear definition of responsibilities and functions for ICT & Security SLOD

IT asset inventory

- ICT & Sec. Risk management connected to the IT Asset inventory

Risk appetite

- ICT & Sec. Risk as a part of risk appetite and risk profile of bank

Spolu sme jedna banka

#prirodzenajlepsi



Changes compared to the current state

Companies are focusing mainly on **IT Security risk + GDPR** category.

The goal is to unify all parts categories as one type of risk:

ICT & Security risk.

IT availability
and continuity

IT Outsourcing

ICT & Sec.
risk

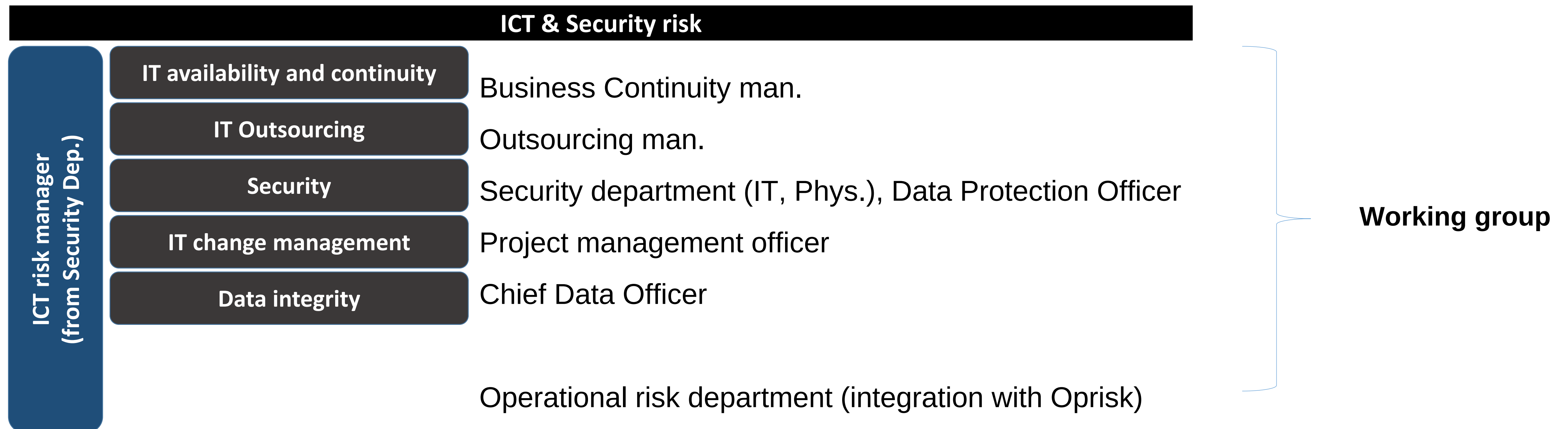
Data integrity

IT Security

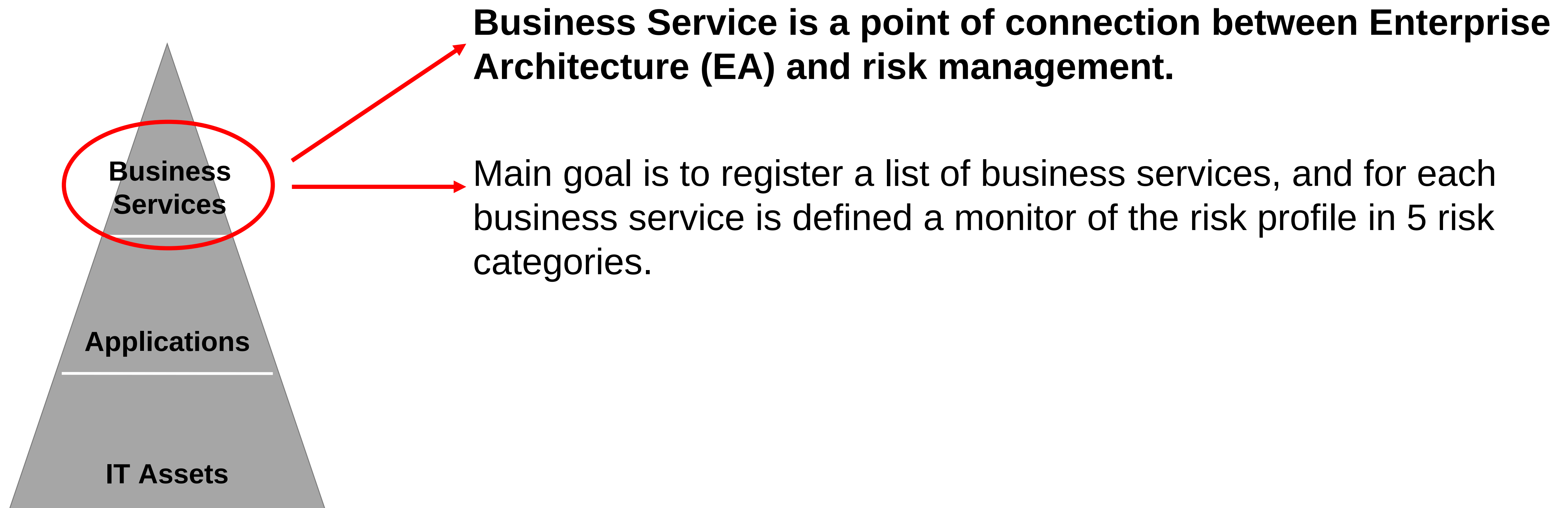
IT change
management

ICT & Security risk committee

ICT & Security risk will be included outside of IT.
Second Line of Defense (SLOD):



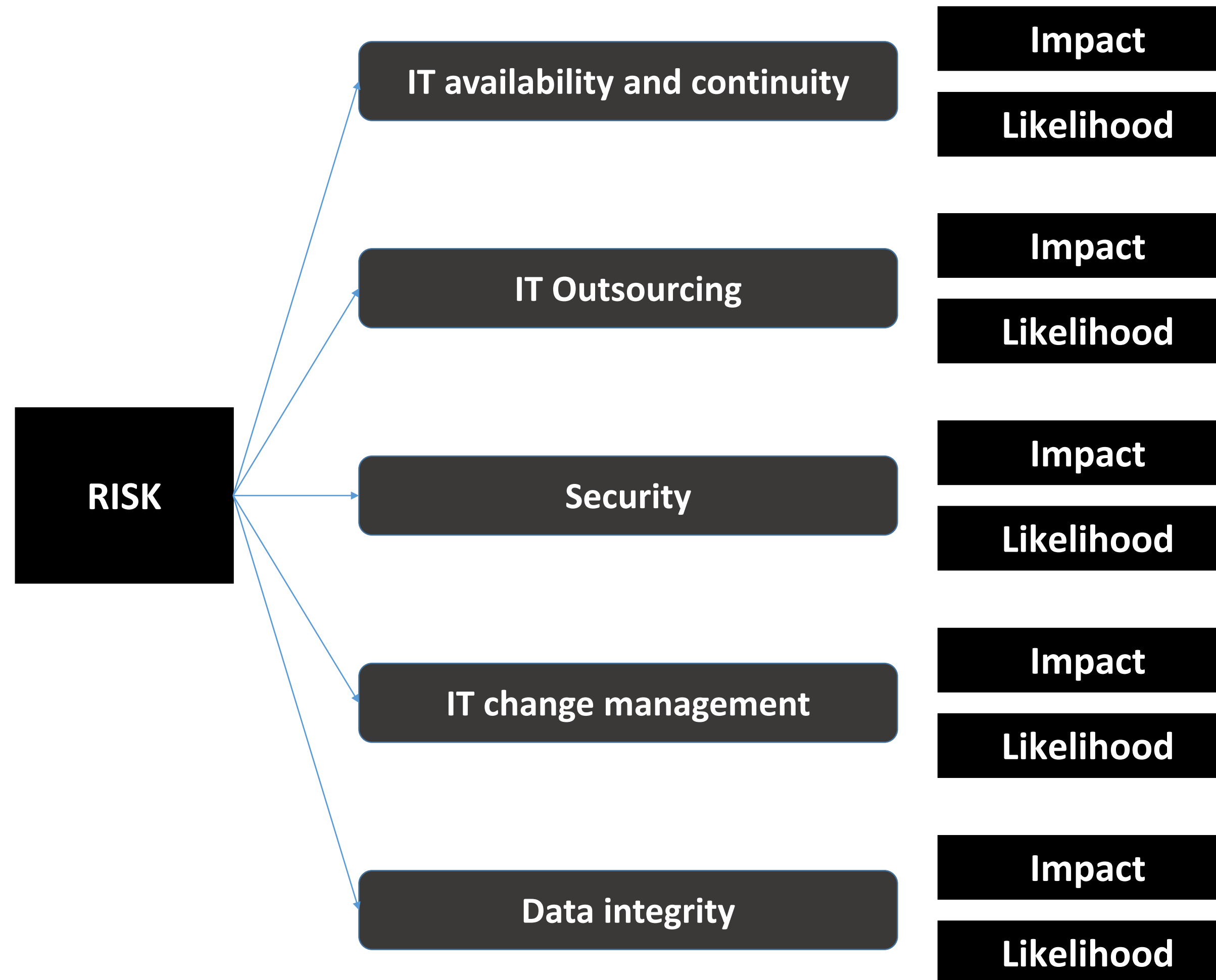
IT asset inventory vs. ICT & Sec. Risk management



Risk assessment – static, dynamic

	Static Risk assessment	Dynamic Risk Assessment
Risk Identificaiton	Regular (annual) assessment, where the predictive risks from the Risk library are evaluated for each Business Service.	Risk are identified: • in SDLC process • Audit findings • Penetration tests • Incidents • Red team tests The identified risks are assigned to the relevant Business service.
Responsibility in TBG	The one risk framework. One management entity ICT & Security risk Council (SLOD)	

Evaluation of risk



Evaluation of risk

IT Risk Register

	Service name	IT risk	Impact					Impact Total	Likelihood	Impact/Likelihood comment	
			Financial	Reputational	Regulatory	Privacy (GDPR)	Business Disruption				Strategic
1	GEOS Service	IT availability and continuity risks	4	3	3	1	2	1	14	3	Financial impact is based on daily average revenue. Likelihood is based on incidents in last 12 months.
2	GEOS Service	IT security risks	2	2	2	1	3	1	11	2	Privacy impact is low because we have no retail customers in the system
3	GEOS Service	IT change risks	1	1	2	1	1	1	7	2	Likelihood is low because the processes are implemented well and controls working efficiently
4	GEOS Service	IT data integrity risks	1	3	3	1	2	1	11	2	Reputational and regulatory effects are considered high, because data is relevant for regulatory reporting
5	GEOS Service	IT outsourcing risks	1	1	3	1	2	1	9	2	Regulatory impact is high because of weak outsourcing procedures are not compliant

Impact table

Likelihood table

Static risk assessment – risk profile of business services

List of Business Services

Business_Service1
Business_Service2
Business_Service3
...

Static Risk Assessment

Business_Service1	IT Availability	Risk 1	Impact: X	Likelihood: Y
		Risk 2	Impact: X	Likelihood: Y
		Risk 3	Impact: X	Likelihood: Y
	Security	Risk 4	Impact: X	Likelihood: Y
		Risk 5	Impact: X	Likelihood: Y
	IT Outsourcing	Risk 6	Impact: X	Likelihood: Y
		Risk 7	Impact: X	Likelihood: Y
	Data Integrity	Risk 8	Impact: X	Likelihood: Y
		Risk 9	Impact: X	Likelihood: Y
	IT Change management	Risk 10	Impact: X	Likelihood: Y
		Risk 11	Impact: X	Likelihood: Y
		Risk 12	Impact: X	Likelihood: Y

Risk Library (Predictive risk)

IT Availability	Vulnerability1 x Threat1 Vulnerability3 x Threat2 ...
Security	Vulnerability4 x Threat1 Vulnerability5 x Threat6 ...
IT Outsourcing	Vulnerability2 x Threat2 Vulnerability3 x Threat3 ...
Data Integrity	Vulnerability4 x Threat1 Vulnerability5 x Threat3 ...
IT Change Management	Vulnerability2 x Threat2 Vulnerability3 x Threat4 ...

OpRisk Integration

Risk appetite

Why is Oprisk integration important?

- It is necessary for integration into risk profile and risk appetite of company.
- The Business services model with EA connection is good premise for Oprisk assessment and more realistic view to IT infrastructure risk profile
- Perfect connection from the high level of business perspective to the technical view on specific vulnerabilities

Every risk in ICT & Security risk will have potential Finance impact

- **Financial Impact as a part of risk appetite in Oprisk reporting**

Oprisk significant risk are managed by Oprisk on company level.

Common risk assessment with business owner (annual)

