SANITA MEIJERE

IT Risk management

The challenge

Almost every business decision requires executives & managers to balance risk & reward.

Effectively managing the business risks is essential to an enterprise's success.

IT Risk underestimation

1

Too often, IT risk (business risk related to the use of IT) is overlooked.

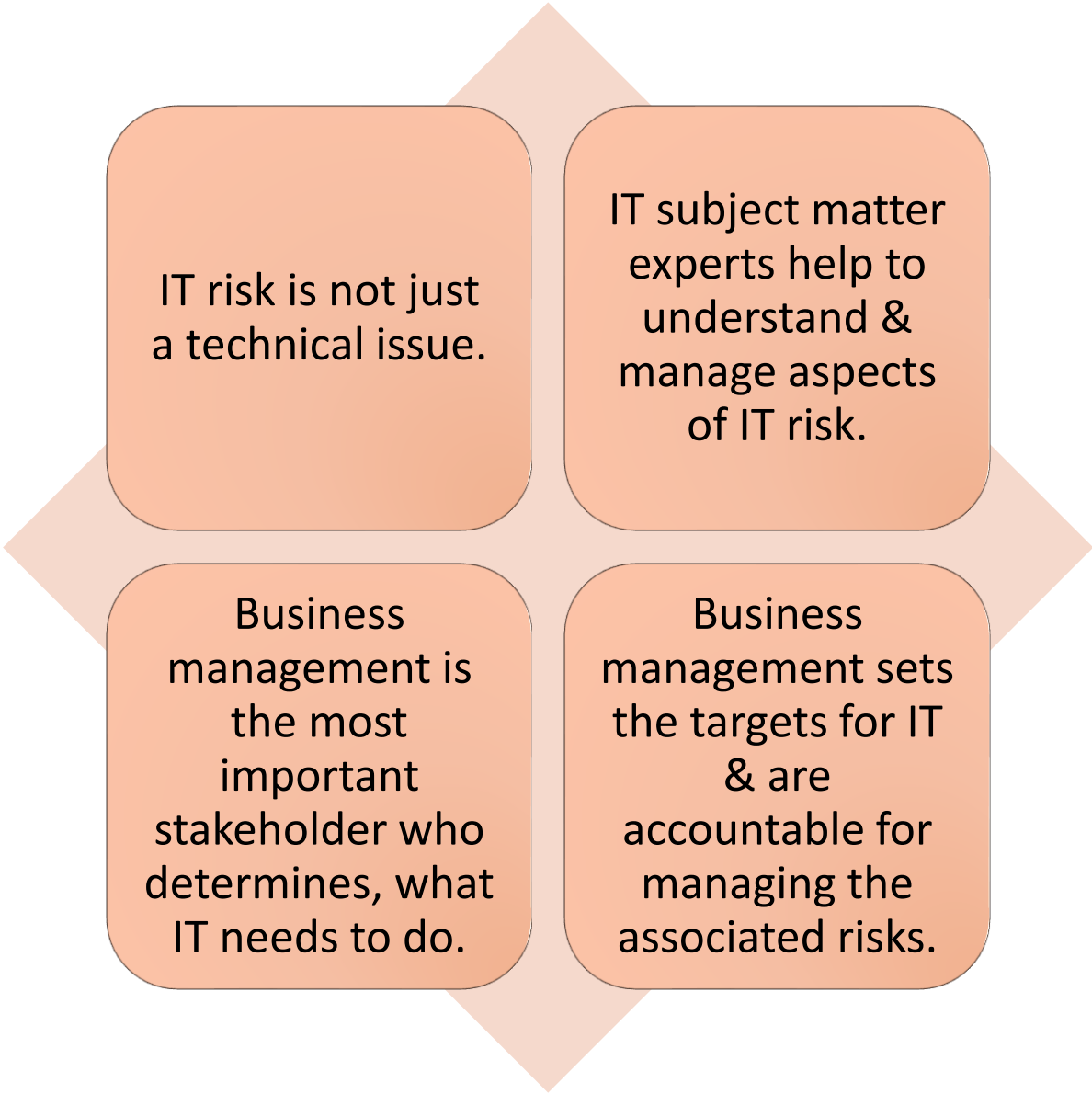
2

IT risk delegated to technical specialists outside the board, despite falling under the same *umbrella* risk category: **failure to achieve strategic objectives.**

3

To prioritize & manage IT risk, Top management needs framework & clear understanding of IT function & IT risk.

IT Risk


IT risk is not just a technical issue.
IT subject matter experts help to understand & manage aspects of IT risk.
Business management is the most important stakeholder who determines, what IT needs to do.
Business management sets the targets for IT & are accountable for managing the associated risks.

Risk IT (ISACA) principles

Always connect risk to business objectives

Balances the costs & benefits of managing IT risk

Promotes fair & open communication of IT risk

Top management support in defining & enforcing personal accountability for operating within acceptable & well-defined tolerance levels

Is a continuous process & part of daily activities

IT Risk management / governance framework

Risk Governance:	Risk evaluation as a process:	Risk Response:
Establish & maintain Common risk view & risk related policies Make risk-aware business decisions	Collect data Analyze risk Maintain risk profile / assessment & treatment plan	Manage risk React to events

Important to remember

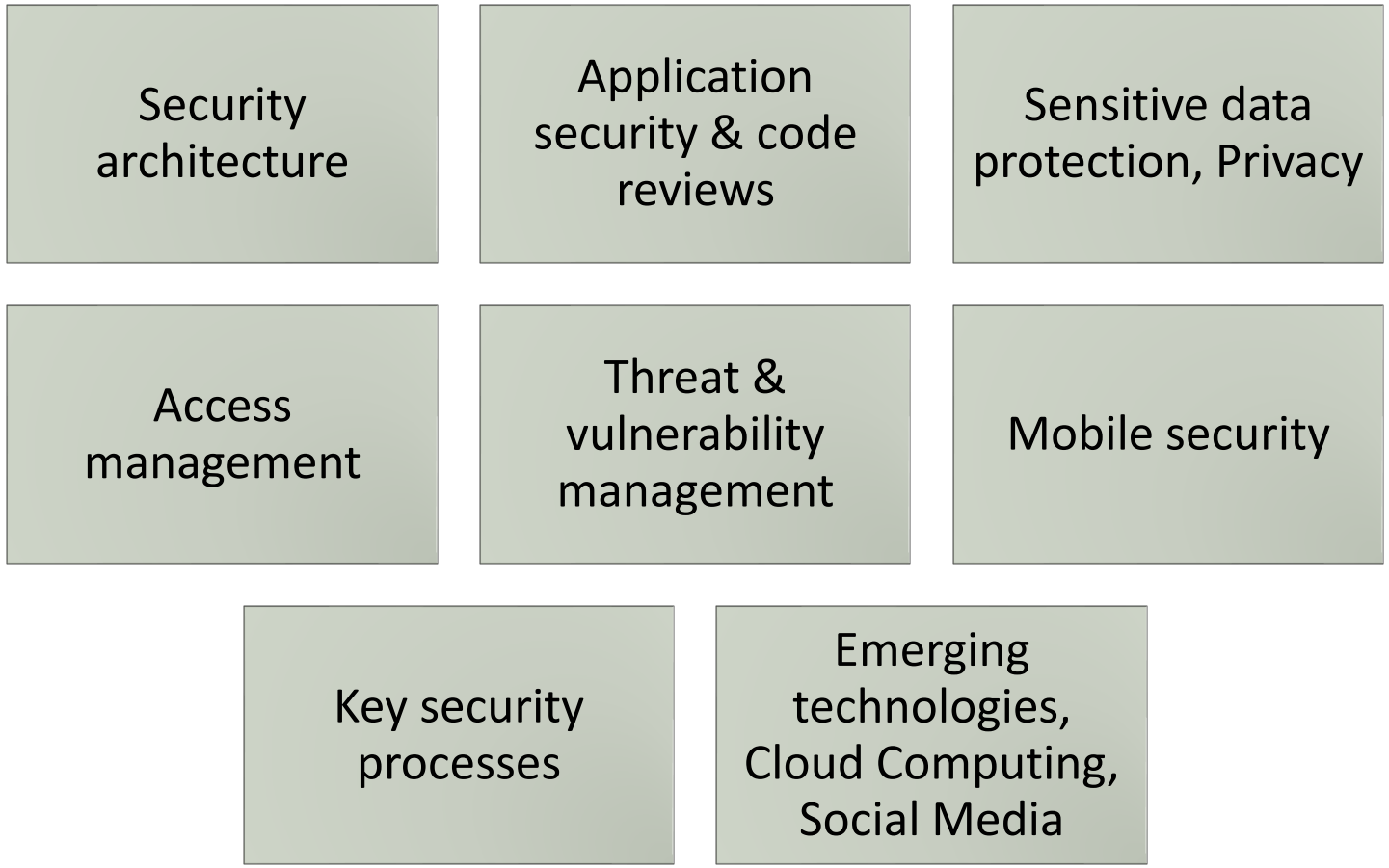
IT risk management does not work *out of the box* - it is not a product to purchase or a policy to put in place.

IT risk management = process of business risk management that must be performed on an ongoing basis.

! Benchmark against industry standards

Risk aware culture = skilled team members who are able to identify, assess threats & perform relevant risk mitigation activities

Key elements in IT risk reduction



Steps to enhance data protection

Risk assessment

Enterprise Data Protection Framework development

Data protection technology deployment

Data classification & ownership

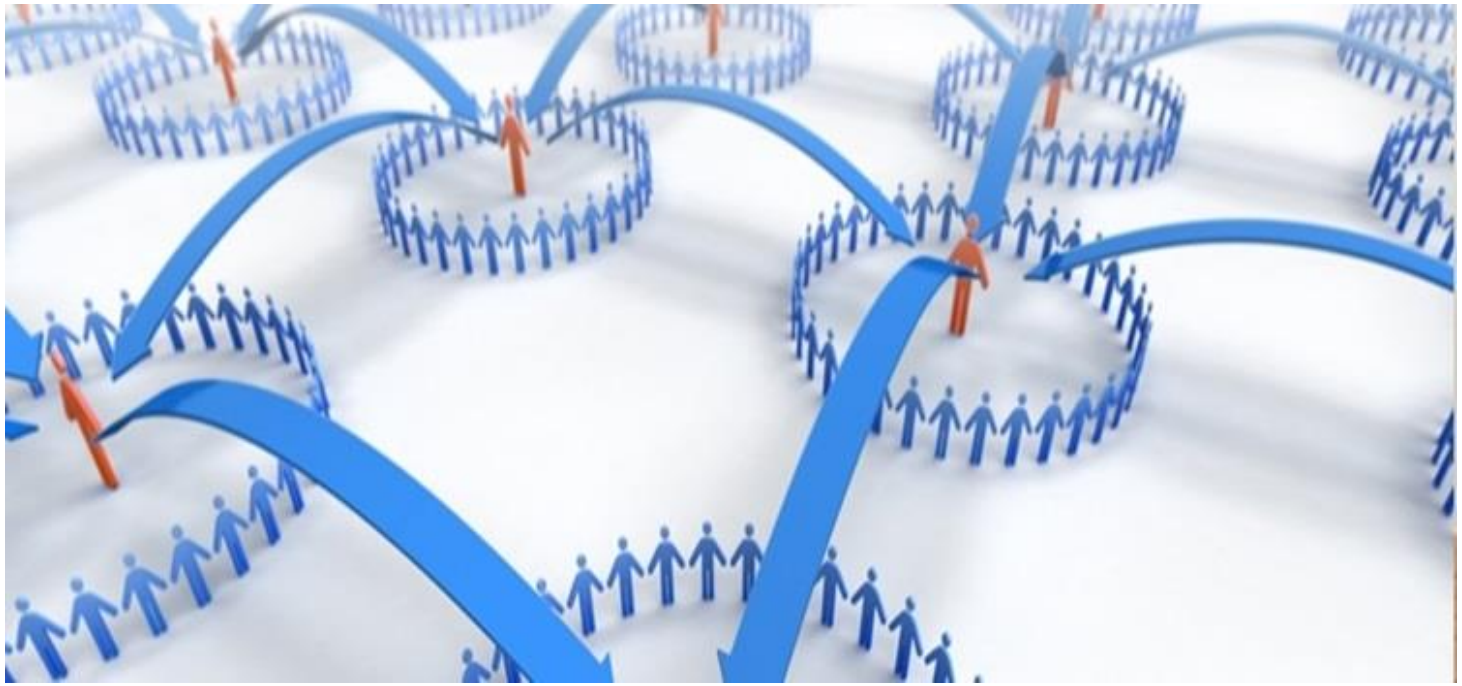
Business process creation

Data breach related risks

- Lawsuits
- Fines
- Compensations
- Regulatory sanctions
- Reputational damage

Disaster recovery plan (DRP)

Activity proactively executed with the goal to recover technology infrastructure (hardware, software, data communications, telecommunications, electronic information assets) from a disaster event & to ensure continuity of operations at established service levels.



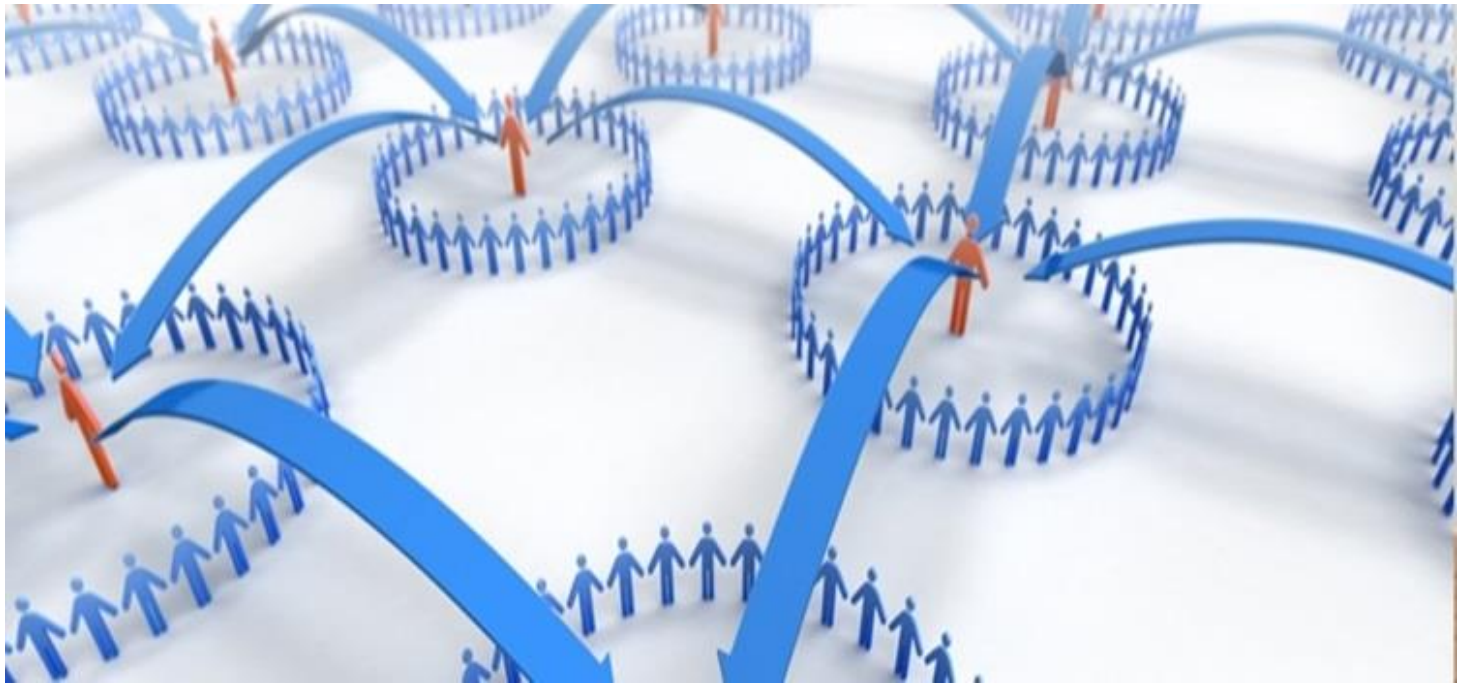
Outsourcing risks I

Weak management / governance (both sides)

Inexperienced staff / turnover / knowledge gap & knowledge transfer

Micro / macro economic uncertainty

Outdated technologies, lost / reduced innovation capacity



Outsourcing risks II

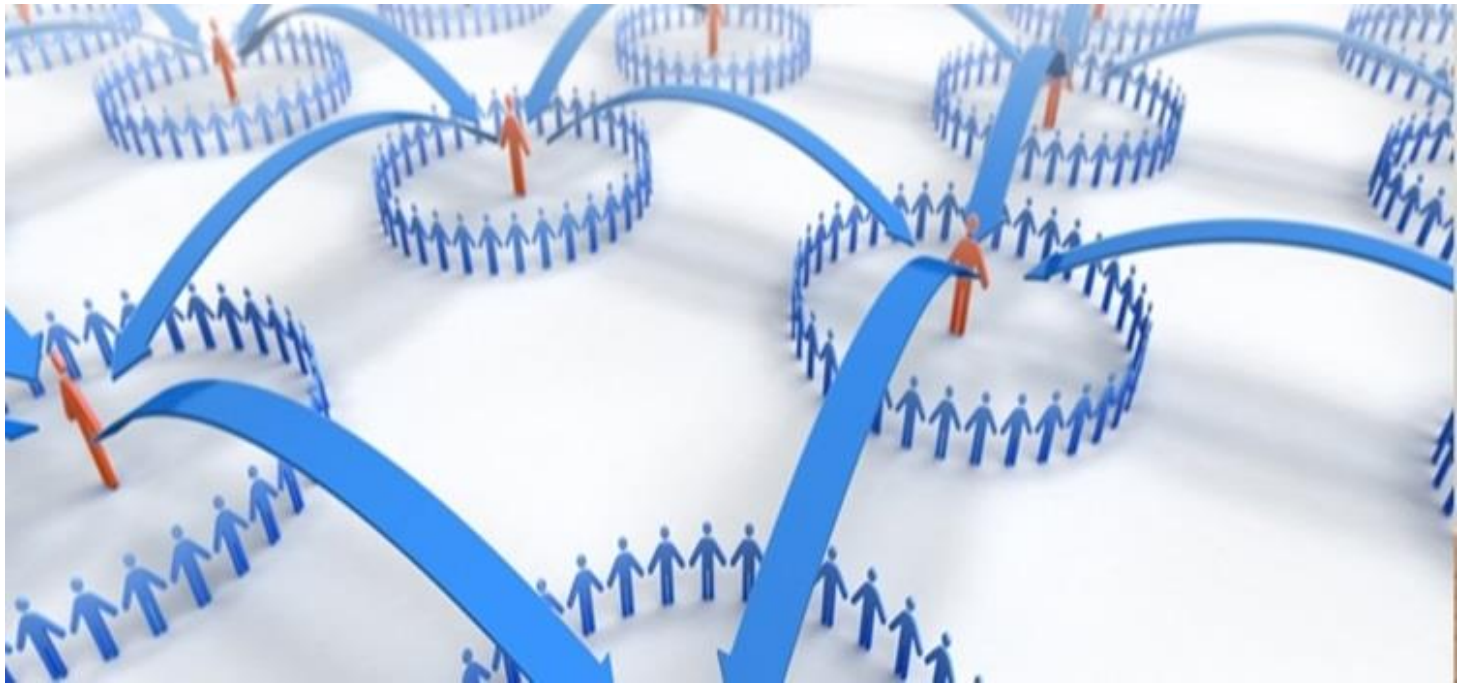
Hidden costs

Loosing knowledge & ability to learn

Communication & relationship & culture

Lower employee morale & productivity

Loss of confidential information



Outsourcing risks III

Operational dependency

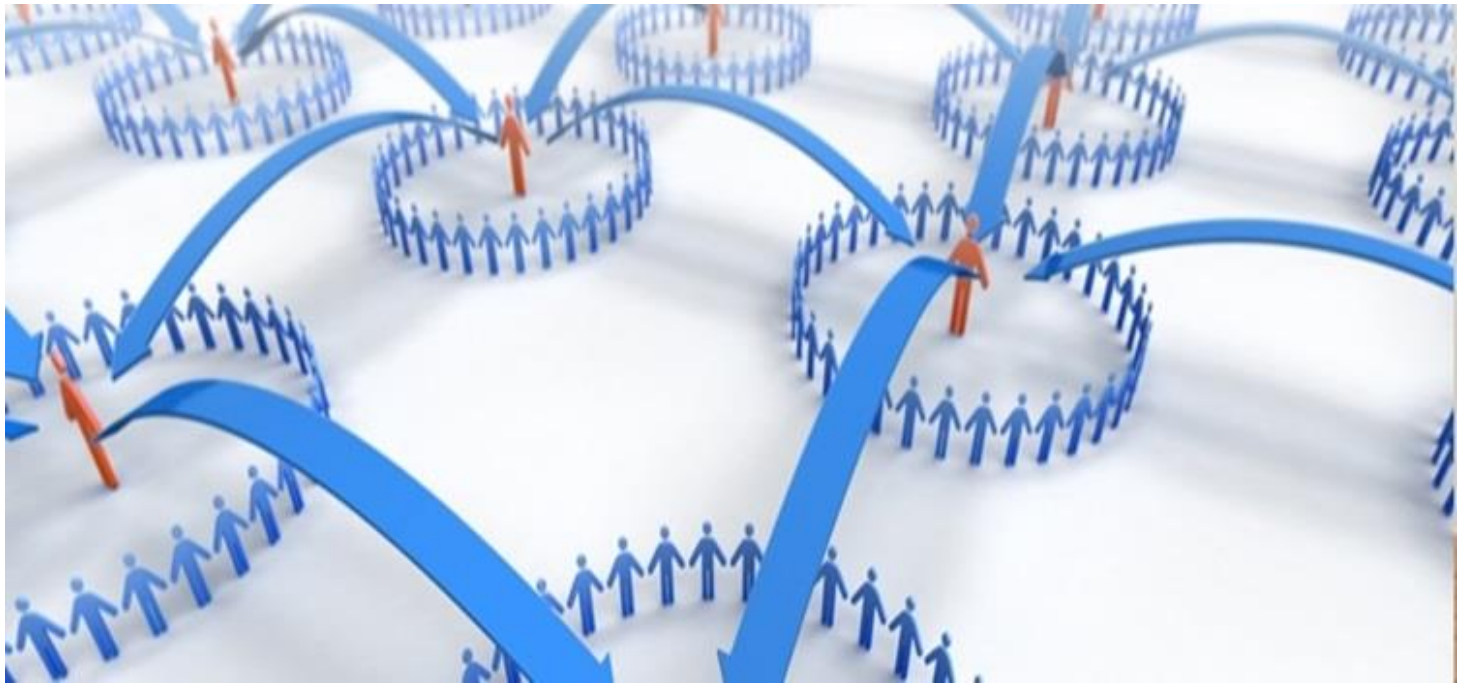
Loss of strategic assets / control over strategic assets

Lock-In

Adoption of disadvantageous architectural style

Wrong competitive signaling

Loss of strategic flexibility



Outsourcing risks IV

Poor / undefined SLAs

Poor / no prioritization

No top management support

Group vs. team

Unrealistic expectations, undefined scope

Bad / no processes (immature process model)

No Quality Assurance

Artificial intelligence (AI) related risks

Creation of *superintelligence* - machines that not only perform narrow tasks that typically require human intelligence (like self-driving cars) but can actually outthink humans.

Early warning from Bil Gates, Steven Hawking, Elon Musk & MIT.

Musk: we needed a direct connection between our brains & our machines to control it. He started *Neuralink* ($100 M investment) aiming to create neural interface by merging computers with human brains.

It becomes serious

4k+ *Google* employees signed a petition protesting $9M AI contract with *Pentagon*. *Google* executives, trying to head off a worker rebellion, said they wouldn't renew the contract when it expires.

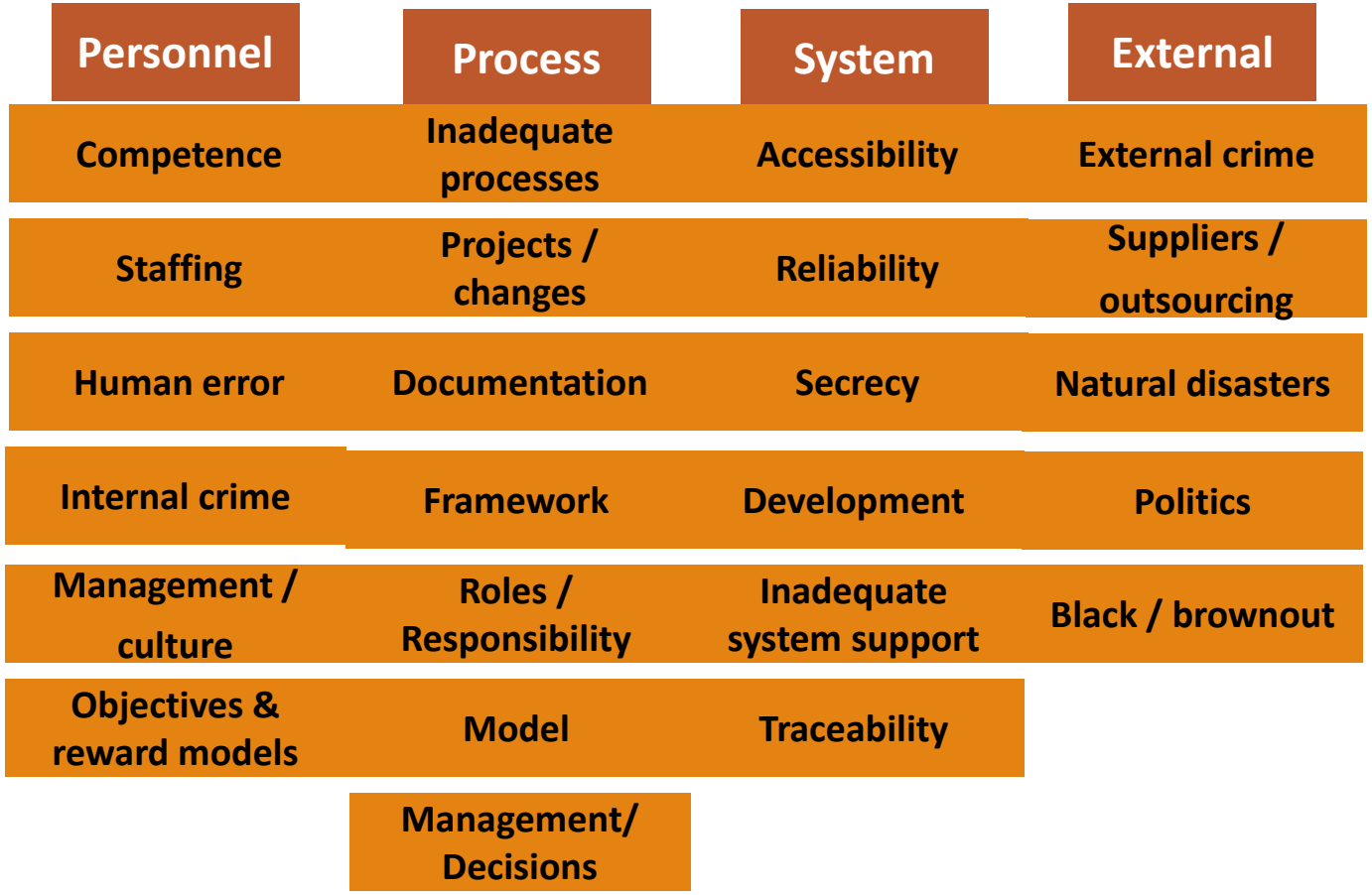
China spends billions to make itself world's leader in AI.

Pentagon is aggressively courting the tech industry

Autonomous weapons are not far away…

We overestimate what can be done in 3 years & underestimate what can de reached in 10 years

To sum up Operational risk structure



IT & systems risks are risks arising from IT & systems inadequacies & Technology-investment.

Accessibility risk: Insufficient access to critical systems, infrastructure / long response times e.g.

- Inadequate maintenance planning, control
- Inadequate capacity planning
- Inaccessible internal network / insufficient connections between systems etc.

Reliability risk: Incomplete, incorrect / inconsistent information e.g.

- Poor control procedures to ensure reliability of transaction data

Secrecy risk: Inadequate protection / handling of confidential information in IT systems e.g.

- Inadequate confidential information protection during transport / storage
- Inadequate / incorrect system authorization

Development risk: Poor procurement, development, design, testing, integration e.g.

- Poor design – no flexible, no user-friendly, no modifiable, no scalable etc.
- Poor testing - unable to detect errors
- Inadequate system documentation

Inadequate system support:

- There is no system support for processes that involve significant manual work
- Inadequate system support for internal control
- Systems that do not support the work process

Traceability: Incorrect / non - complete tracking of information in IT system.

- Lack of information concerning who has made transactions, what has been done &when

Useful frameworks

COBIT provides a set of controls to mitigate IT risk = the means of risk management.

Risk IT (ISACA) provides a framework for enterprises to identify, govern & manage IT risk.

Thank you!
Q&A