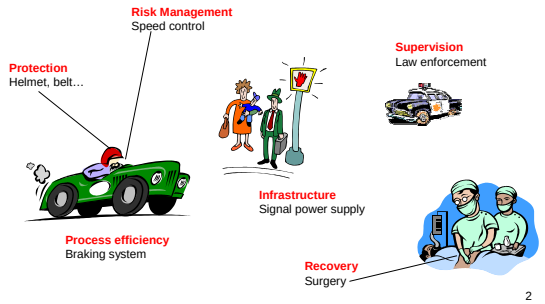
3. Risk Management

2005

Road Safety
An Example of Complex Improvement



2

The Risk Chain

Hazard	Exposure	Resiliency	Contingency
• Prevention • Detection • Surveillance	• Risk Control • Protection • Insurance	• Reactivity • Robustness • Adaptability	• Restore • Repair • Adapt

Minimise probability of event — **Minimise damage if event happens** — **Cope with the damage caused by the event**

3

Mis on risk?

Riskina mõistame me ebasoovitava sündmuse ilmnemist.

Riski iseloomustavad tõenäosus ja mõju - seega on riski rahaline väljendus funktsioon ebasoovitava sündmuse tõenäosusest ja sündmusega kaasnevast kahjusummast.

4

Riskide tüübid

- Krediidirisk
- Tururisk
- Operatsioonirisk
- ...

5

Operational Risk Is Integral To Enterprise Risk Management

6

OR and Operational Excellence

- From an operating standpoint, these challenges require a cross-enterprise excellence in at least 3 areas
  - technology infrastructure
  - business process architecture
  - business process integration
- Efficiency and resilience are two sides of the same coin
  - For each $ spend on projects, there is an optimum balance between efficiency and resilience improvement objectives

7

Risk Sources Ordered by Importance

1. Lack of top management commitment
2. Failure to gain user commitment
3. Misunderstanding of requirements
4. Inadequate user involvement
5. Failure to manage end-user expectations
6. Changing scope and/or objectives
7. ….

8

Greater Risk of IT Failure

- Business transactions are increasingly dependent on IT, so failures in IT are more likely to impact the business, and that impact is more likely to be severe.
- The IT environment is increasingly complex, so even if the environment stays the same size, the number of potential failure points is rising.
- IT directly controls less of the infrastructure (*"virtual IT environment"*), so managing the possibility of failure is more important because IT has less ability to react after the failure occurs.
- When an IT failure occurs, there is less time between the failure and its impact on the business.
- IT failures are increasingly visible outside the data center, so more people react negatively when a failure occurs.

9

Greater Risk of IT Failure

- IT today has more potential to enable business than ever before, but failures in IT have more potential to *disable* business.
- At the same time, the traditional risk management strategy of tight change control is less often available, and less often effective.

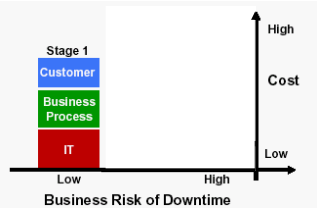
10

IT Downtime

- IT downtime joins other natural disasters in business **risk management**.
- As IT "becomes" the facility, it is going to raise new, unheard of risks.
  - *A slow Web site could be as disastrous as a tornado.*

11

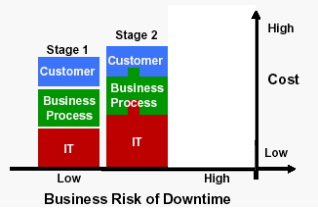
IT Downtime



In a Stage 1 enterprise, the interdependencies of business processes, IT and external entities are managed by manual or non-IT interfaces. Thus, if an IT system is not available, it is not apparent to customers or the supply chain, and the business can muddle along until the computers are fixed.

12

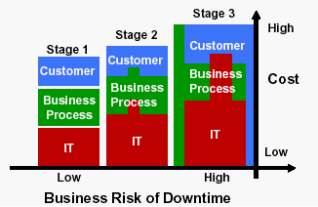
IT Downtime



In Stage 2, IT has permeated the business processes, so when the computers are down, the business processes come to a halt. This inherently brings more business risk to the enterprise. Most large enterprises have created some level of dependency between business processes and IT (any ERP, HR, integrated financials or sales management system creates this business/IT process interdependency).

13

IT Downtime



In stage 3, where enterprises will be during the next five years, the business risk of IT is maximum. The cost of maintaining the integrity of these systems will be huge, but the cost of downtime will be even greater. There has never been a more critical time for massive efficiency in IT systems.

14

IT Downtime

- IT is permeating the entire business function.
- IT is inextricably linking customers, suppliers, business partners and government into a seamless continuum of business activity.
- There are no insulating layers, where a functional failure in one aspect of the business can be an isolated incident.
- Not only are business processes interrelated, they are becoming interdependent.

15

Threats to the Information Systems

- **Availability** - This is broadly defined as having the resource in a given place, at the given time, and in the form needed by the user.
- **Confidentiality** - Some define this as "The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations".
- **Integrity** - One can define this as "The ability of an AIS to perform its intended function in a sound, unimpaired manner."
- The replacement cost
- The cost to recreate intellectual property
- The value of an hour of computing time.
- Other considerations (embarrassment, loss of confidence,…)

16

Implications

- Risk management should be integrated into operations decision making in every job function and every role.
- Risk management should be taken seriously and given an appropriate amount of effort.
- Risk management should be done continuously to ensure that operations is dealing with the risks that are relevant today, not just the ones that were relevant last quarter.

17

Characteristics of Risk

- **Risk is a fundamental part of operations.** The only environment that has no risk is one whose future has no uncertainty: no question of whether or when a particular hard disk will fail; no question of whether a Web site's usage will spike or when or how much; no question of whether or when illness will leave the help desk short-staffed. Such an environment does not exist.
- **Risk is neither good nor bad.** A risk is the possibility of a future loss, and although the loss itself may be seen as "bad," the risk as a whole is not. It may help to realize that an opportunity is the possibility of a future gain. There is no risk without opportunity, and no opportunity without risk.
- **Risk is not something to fear, but something to manage.** Because risk is not bad, it is not something to avoid. Operations teams deal with risks by recognizing and minimizing uncertainty and by proactively addressing each identified risk. If a loss is one possible future outcome, then the other possible outcomes are gains, smaller losses, or larger losses. Risk management lets the team change the situation to favor one outcome over the others.

18

Principles of Successful Risk Management

- **Assess risks continuously.** This means the team never stops searching for new risks, and it means that existing risks are periodically reevaluated. If either part does not happen, risk management will not benefit the company.
- **Integrate risk management into every role and every function.** At a high level, this means that every IT role shares part of the responsibility for managing risk, and every IT process is designed with risk management in mind. At a more concrete level, it means that every process owner:
  - Identifies potential sources of risk.
  - Assesses the probability of the risk occurring.
  - Plans to minimize the probability.
  - Understands the potential impact.
  - Plans to minimize the impact.
  - Identifies indicators that show the risk is imminent.
  - Plans how to react if the risk occurs.

19

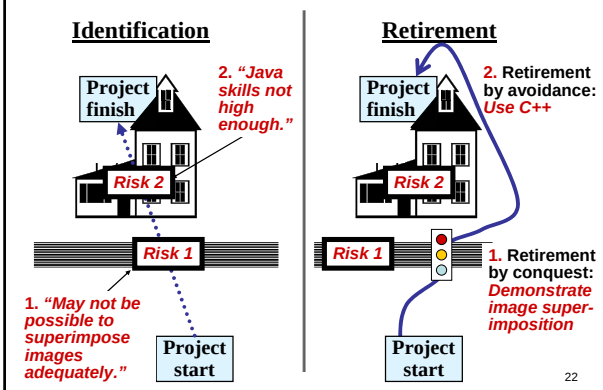
Principles of Successful Risk Management

- **Treat risk identification positively.** For risk management to succeed, team members must be willing to identify risk without fear of retribution or criticism. The identification of a risk means the team faces one less unpleasant surprise. Until a risk is identified, the team cannot prepare for it.
- **Use risk-based scheduling.** Maintaining an environment often means making changes in a sequence, and where possible the team should make the riskiest changes first. An example is beta-testing an application. If the company wants 10 features to work, and two of them are so important that the lack of either would prevent the application's adoption, test those two first. If they were to be tested last and either was to fail, then the team would have lost the resources invested in testing the first eight.
- **Establish an acceptable level of formality.** Success requires a process that the team understands and uses. This is a balancing act. If the process has too little structure, people may use it but the outputs won't be useful; if it is too prescriptive, people probably won't use it at all.

20

Risk Management Process

The Risk Management Mindset



22

Compute risk priorities (*example*)

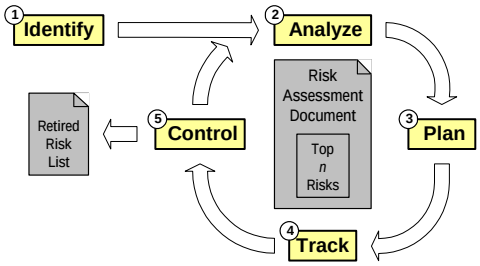
	Likelihood 1-10 *1 = least likely*	Impact 1-10 *1 = least impact*	Retire-ment cost 1-10 *1 = lowest retirement cost*	Priority computation	Resulting priority *Lowest number handled first*
The highest priority risk	**10 (most likely)**	*10 (most impact)*	1 (lowest retirement cost)	(11-**10**) *(11-*10*) *1	**1**
The lowest priority risk	**1 (least likely)**	*1 (least impact)*	10 (highest retirement cost)	(11-**1**) *(11-*1*) *10	**1000**

Sample Risk Analysis

#	Risk title (details given above)	Like-lihood 1-10 *1=least likely*	Im-pact 1-10 *1=least impact*	Retire-ment cost 1-10 *1=lowest retirement cost*	Pri-ority *lowest number handled first*	Retirement / mitigation plan	Respon-sible engineer	Target com-pletion date
1	Super-imposing images	3	10	1	8	Experiment with Java images.	P. R.	12.01.05
2	Deficient Java skills	9	6	8	80	H.T., K.M., V.I. and L.D. to attend training course beginning 1/5/05 at Ultra Training Corp, obtain Java level 2 certification by 3/1/05 and level 3 certification by 4/1505	H. L.	14.04.04
3	Alan Gray may be pulled off this project	3	7	9	288	Susan Ferris to inspect all of Alan's work	S.F.	Contin-ual
.	...	...	...	...	...	...	...	...

24

Process Overview - the proactive risk management process



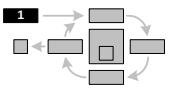
25

Five Steps of Risk Management

- Step 1: Risk Identification
- Step 2: Risk Analysis
- Step 3: Risk Action Planning
- Step 4: Risk Tracking
- Step 5: Risk Control

26

Step 1: Risk Identification



- Team identifies the components of the risk statement:
  - Condition
  - Operations consequence
  - Business consequence
  - Source of risk
  - Mode of failure

27

Riskide identifitseerimine

Kui sa ei tea mida pead juhtima, siis sa ei saa ju juhtida …

-kontrollikeskkond

-tegijad on eksperdid

Kui enda teadmistest jääb puudu, siis kasutatakse ka väliseid eksperthinnanguid (due diligence, risk surveys, ...)

28

Source of Risk

- **People.** Everyone makes mistakes, and even if the group's processes and technology are flawless these human errors can put the business at risk.
- **Process.** Flawed or badly documented processes can put the business at risk even if they are followed perfectly.
- **Technology.** The IT staff may perfectly follow a perfectly designed process, yet fail the business because of problems with the hardware, software, and so on.
- **External.** Some factors are beyond the IT group's control but can still harm the infrastructure in a way that fails the business. Natural events such as earthquakes and floods fall into this category, as do externally generated, man-made problems such as civil unrest, computer virus attacks, and changes to government regulations.

29

Risk factors

- Project risks
- System/Technology Risks

30

Project risks

- Scope creep
- Cost/time overruns
- People

31

System/Technology Risks

- Downtime risks
- Performance risks
- Installation/deployment risks
- Support risks
- Infrastructure integration/interoperability risks
- Standards risks
- Communications risks
- Training risks

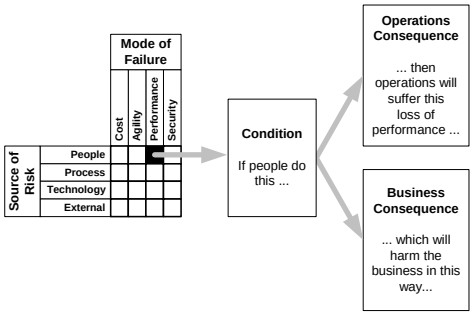
32

Mode of Failure

- **Cost.** The infrastructure can work properly, but at too high a cost, causing too little return on investment.
- **Agility.** The infrastructure can work properly, but be unable to change quickly enough to meet the business needs. Capacity problems are the most obvious case.
  - For example, someone might have a dozen new servers ready to support increased processing needs, but forget that the cooling systems in the data center were already at peak capacity, and upgrading those systems will take a month.
- **Performance.** The infrastructure can fail to meet users' expectations, either because the expectations were set wrong, or because the infrastructure performs incorrectly.
- **Security.** The infrastructure can fail the business by not providing enough protection for data and resources, or by enforcing so much security that legitimate users can't access data and resources.

33

The risk statement



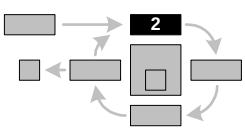
34

Risk Statement Form

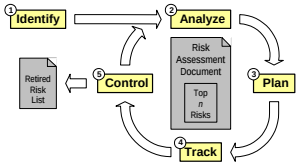
- **Role or function.** The service management function most directly involved with the risk situation.
- **Risk context.** A paragraph containing additional background information that helps to clarify the risk situation.
- **Related risks.**

35

Step 2: Risk Analysis



- ***Risk Probability***
- ***Risk Impact***
- ***Risk Exposure*** - is the result of multiplying the probability by the impact



36

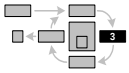
Riskide analüüs

Kui oled riskid identifitseerinud, siis

- tõenäosuse mõõtmine
- mõju hindamine

37

Step 3: Risk Action Planning



Mitigations

- **Reduce.** Risk reduction minimizes the risk's probability or its impact, or both. For example, redundancy generally reduces the impact of failure. If one component fails there is no impact because the redundant component is still working. Keeping track of those components' expected lifespan and replacing them before they're expected to fail reduces the probability of the failure. Ideally, a reduction method reduces probability or impact to zero, but this is not always possible.
- **Avoid.** Risk avoidance prevents the team from taking actions that increase exposure too much to justify the benefit. An example is upgrading an unimportant, rarely used application on all 50,000 desktops of an enterprise. In most cases, the benefit doesn't justify the exposure, so IT avoids the risk by not upgrading the application.
- **Transfer.** Whereas the avoidance strategy eliminates a risk, the transference strategy often leaves the risk intact but shifts responsibility for it to another group. For example, a company with an e-commerce site might outsource credit verification to another company. The risks still exist, but they become the outsource partner's responsibility. However, if the outsource partner is better able to perform credit verification, then transferring the risks can also reduce them.

38

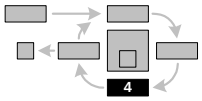
RISKIDE leevendamine

Kui riski rahaline väljendus on leitud, küsime endalt:

- kes teeb otsuse?
- strateegia kujundamine
    - kas risk on aktsepteeritav?
    - kas tänane riskijuhtimise tase on piisav?
    - on veel midagi vaja ette võtta?
- tegevusplaan maandamiseks
    - vastavuses defineeritud riskiprofiiliga
    - kuluefektiivne

39

Step 4: Risk Tracking



This step monitors three main changes:

- **Trigger values.** If a trigger becomes true, the contingency plan needs to be executed.
- **The risk's condition, consequences, probability, and impact.** If any of these change (or are found to be inaccurate), they need to be reevaluated.
- **The progress of a mitigation plan.** If the plan is behind schedule or isn't having the desired effect, it needs to be reevaluated.

40

Monitooring

Peale riski leevendamise tegevuste elluviimist:

- kas nüüd on risk aktsepteeritaval tasemel?

- kontrollikeskkond - kas saame tegijaid usaldada või peame auditeerima?

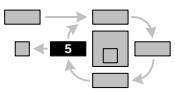
- riskide kontrollide testimine

- **riski indikaatorid**

- tagasiside

41

Step 5: Risk Control



The controlling step executes a planned reaction to the change:

- If a trigger value has become true, then execute the contingency plan.
- If a risk has become irrelevant, then retire the risk.
- If the condition or a consequence has changed, then redirect to the identification step to reevaluate that element.
- If the probability or impact has changed, then redirect to the analyzing step to update the analysis.
- If a mitigation plan is no longer on track, then redirect to the planning step to review and revise the plan.

42

Kontroll

Riski indikaatorid

Riski indikaatorid on ettevõtte erinevaid valdkondi iseloomustavad arvulised suurused, mis korreleeruvad riski suurusega.

Me kasutame neid indikaatoreid kui varase hoiatuse signaale. Siinjuures on tähtsaim mitte mingi näitaja absoluutväärtus vaid selle trend.

Näited - personali voolavus, motivatsiooni tase, IT süsteemide maasoleku aeg, mitteresidentidest klientide arv, väljamüüdud teenuste maht, …

… aga ka makromajanduse näitajad nagu jooksevkonto defitsiit, tööpuuduse tase, keskmise palga kasv jms

43

Risk Analysis Template

Activity	Risk of Damage			Magnitude of Damage			Planned Action	
	Low	Medium	High	Low	Medium	High	No Action	Type of Action

44

Riskide juhtimise meetodid

Information Security Expenditures

- % of passwords cracked via password cracking tools;
- % of production environments not separate from test environments;
- number of hours/days needed to recover from an incident;
- number of months since last InfoSec policy review;
- % of applications/environments with no audit trail;
- % of desktops/servers with old virus signature files;
- % of access requests received outside of the normal request process;
- % of user password resets done by help desk;
- % of development personnel having access to production
- % of servers not in physically secure rooms;environment;

46

Metrics information security policies.

- Establish critical effectiveness metrics for each information security policy.
- Ensure audit logs are in place for all mission-critical applications and systems.
- Begin moving toward a centralized log entries.

47

Riskide juhtimise meetodid

RISKI TÜÜP	MEETODID
Töötaja pettus	Funktsioonide lahusus Kuritegevuse kindlustus Tehingulimiidid Allkirjaõiguste limiidid
Töötaja eksimus	Topeltkontroll Vastutuskindlustus
Väline kuritegevus	Turvaseadmed Klientide identifitseerimine
Koostööpartnerite risk	Partnerite due diligence Lepingute due diligence Talitluspidevuse planeerimine
Elektrooniline kuritegevus	Tehingulimiidid Programmiõiguste administreerimine Arvutitöökohtade kaitse pealtkuulamise eest
IT riskid	Andmete dubleerimine Riistvara dubleerimine Võtmeisikute dubleerimine Teenuse sisseostmine Andmeside krüpteerimine
Juriidilised riskid	Lepingute due diligence
Füüsilised katastroofid	Varakindlustus

48

Riskide juhtimise meetodid

Riskijuhtimise meetodid on praktilised tegevused ja abinõud mida kasutatakse kokkulepitud strateegiate elluviimiseks.

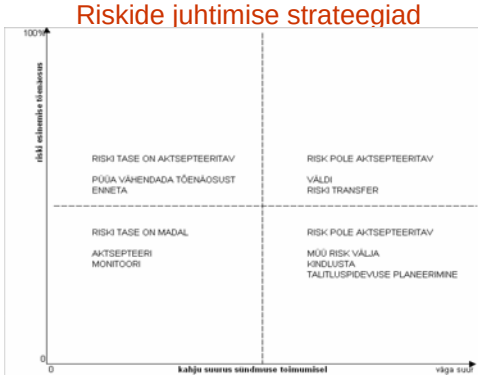
Kõige olulisemad ja efektiivsemad meetodid:

- duaalsus
- funktsioonide lahusus
- tehingulimiidid
- varukoopiad
- back-up süsteemid
- dokumenteerimine
- riskiteadlikkuse tõstmine
- kindlustus

49

Riskide juhtimise strateegiad

Riskide juhtimise strateegiad



51

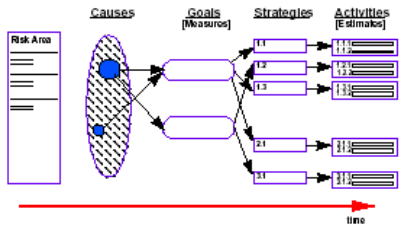
Riskide juhtimise strateegiad

Riskijuhtimise strateegia on sisuliselt otsus selle kohta, mida me selle riskiga ette peaksime võtma. On neli peamist strateegiat:

- leevendamine (=optimeerimine)
- aktsepteerimine
- vältimine (=minimeerimine)
- välja müümine (=transfer, finantseerimine)

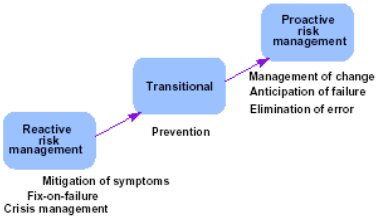
52

Mitigation Strategy Planning (MSP)



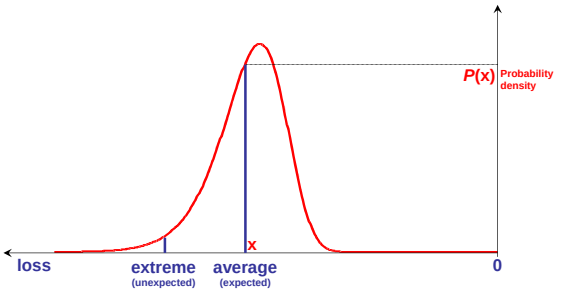
53

Approaches to Risk Management



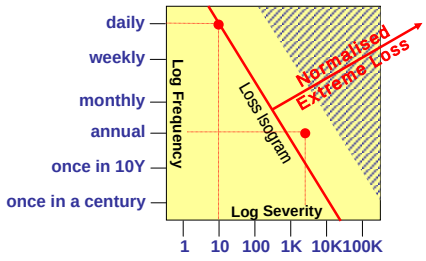
54

Risk Management and Insurance



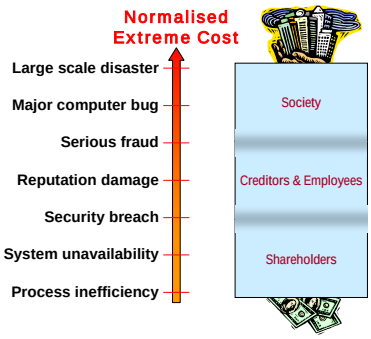
55

How Much Can You Afford?



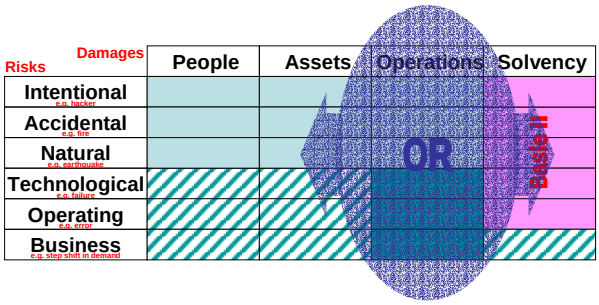
56

Who Cares?



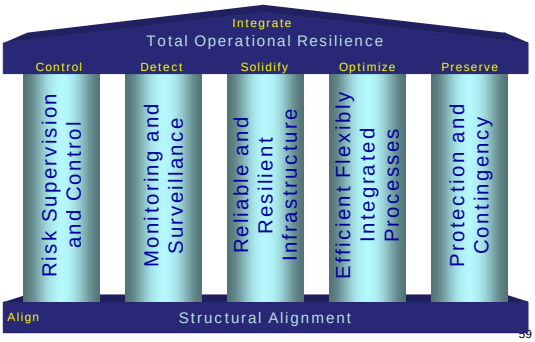
57

Initiative Focus versus Risk Sources



58

Operational Resilience



59

Operational Resilience: A New Step for Technology

- Increased sophistication of both businesses and systems has created vulnerabilities in our modern communication, co-operation and information-based economies.
- We have made our information technology incredibly powerful, fast, and reliable. Now, in order to contain the risks technology complexity and dependency have generated within acceptable levels, we need it to be resilient.
- Operational Resilience is the ability of systems, resources and processes to effectively support a business under any sudden adverse or unexpected condition.
- The IBM Operational Resilience Solution™ is a set of offerings, techniques and capabilities whose aim is to maximize the Operational Resilience of organisations, considered within their network of inter-dependencies.

60

Towards Maximal Resiliency

61

OR as a major challenge for Institutions

- Improve efficiency
  - Implement end-to-end automation
  - Optimise cost structure and effectiveness
  - Optimise resource allocation
- Improve "agility" (dynamic differentiation)
  - Leverage knowledge and relationships
  - Optimise value-chains and value-nets
  - Dynamically adapt to environmental and strategic changes
- Improve resilience
  - Manage operational risks
  - Reduce overall business vulnerability
  - Develop capabilities to quickly adjust, adapt, or switch operating mode when circumstances require

… under increased resource constraints

62

Näide: Eesti Ühispank

Operatsioonirisk

- Operatsiooniriski all mõistetakse riski, mis sisemiste (ebaefektiivsed protseduurid, puudulikud infosüsteemid, personali pädevus ja lojaalsus jne.) või väliste (reputatsiooni langus, kriminaalsed aktid, katastroofid) tegurite mõjul võib häirida panga äritegevust või viia ootamamtute kahjumite tekkeni.
- Ebaefektiivsetest protseduuridest tuleneva riski maandamiseks kasutab pank standardset protseduuri, mis peab tagama toote igakülgse kaetuse lepingute (juriidiline risk), kontrolltoimingute ja tõese raamatupidamisliku kajastamisega. Peale toote juurutamist viib sisekontrolli osakond regulaarselt läbi kontrolle kehtestatud protseduurist kinnipidamise tagamiseks. Operatsioonirriskide kvantifitseerimiseks tulevikus töötab riskijuhtimise osakond erinevate metoodikate kallal, uurides võimalusi nende kohaldamiseks kohalikele oludele.
- Eesti Ühispanga suhtes kehtivad Skandinaviska Enskilda Banken AB poolt sõlmitud ja SEB tütarettevõtjatele laienevad kindlustuslepingud, millega on kindlustatud:
  - panga töötaja või kolmanda isiku poolt toime pandud kuriteo tagajärjel (nt. võltsimine, röövimine, vargus, kelmus) tekkinud varaline kahju;
  - panga igapäevase majandustegevuse käigus panga töötaja hooletuse, vea või tegevusetuse tõttu tekkinud varaline kahju;
  - panga juhatuse liikme või töötaja ebaseadusliku teo tagajärjel tekkinud kahju;
  - panga tegevuse tõttu kolmandale isikule tekkinud kahju.

64

Infotehnoloogilised riskid

- **Infotehnoloogiliste riskide juhtimise eesmärk:**
- on Eesti Ühispanga informatsiooni turvalisuse tagamine ning sellega seoses panga ärikriitiliste protsesside katkemist ja ärikahjude tekkimist tingivate turvasündmuste vältimine.
- **Infotehnoloogiliste riskide juhtimise organisatsioon.** Eesti Ühispanga *Operatsiooniriskikomitee* on Eesti Ühispanga turvatööd, tehnoloogilise kvaliteeti juhtimise ning *tehnoloogiliste riskide* hindamist suunav ja koordineeriv organ, mis tegutseb Eesti Ühispanga Juhatuse poolt antud volituste piires.
- ÜP andmeturbe grupp tagab riskide hindamise ja juhtimise IT valdkonnas.
- **Eesti Ühispanga IT infrastruktuur.**
- Eesti Ühispanga IT infrastruktuur tagab Eesti Ühispanga andmete ja infosüsteemide turvalisuse vastavate tehnoloogiliste meetmete (tulemüürid, ründetuvastus ja –peletus, viirusekaitse, pääsupoliitika rakendamine jmt) rakendamisega.

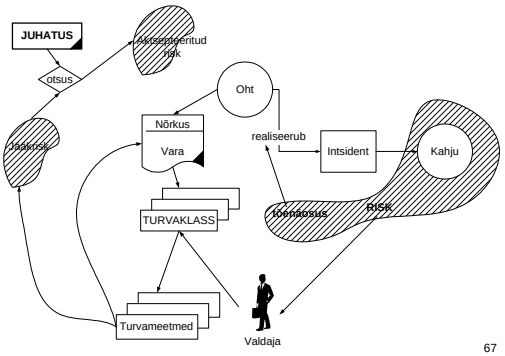
65

Infotehnoloogiliste riskide analüüs

- Eesti Ühispanga Operatsiooniriski poliitika realiseerub riskianalüüsi põhjal kehtestatud turvanõuetele vastavate turvameetmete rakendamise kaudu.
- Kõikide uute pangatoodete evitamisele eelneb nende toodete infotehnoloogiliste riskide analüüs, vajaduse korral modifitseeritakse toote infotehnoloogilist tuge nii, et toode vastaks tarvilikule turvatasemele. Infoturbe projekteerimine koosneb järgmistest etappidest:
  - Infovarade ja nende valdajate määramine
  - Infovarade turvanõuete määramine
  - Jäme riskianalüüs
  - Turvameetmete määramine – vajaduse korral detailne riskianalüüs ja turvameetmete täsustamine
  - Jääkriskide aktsepteerimine
  - Infoturbe käigushoid:
  - Muudatuste/intsidentide seire/haldus
  - Infoturbe perioodiline akrediteerimine
  - Infoturbe intsidentide käsitlemine

66

Kokkuvõte



67