



*Nature
at work*

IT-Security policy and Risk Management



Statkraft

IT-Security IS Risk Management
IT-Security IS Risk Management



*Nature
at work*

Agenda – What will this session cover

Framework

- **'Make it personal' is the reason and basis for Statkraft implementation of Risk Management**

Security policy importance and function

- **Security policy is reduced to standards and central security roles by introduction of risk management**

Distributed security governance

- **The customer takes responsibility for risk and consequence of threats caused by IT services**
- **IT product managers are responsible for communicating threats and their probability of occurrence**

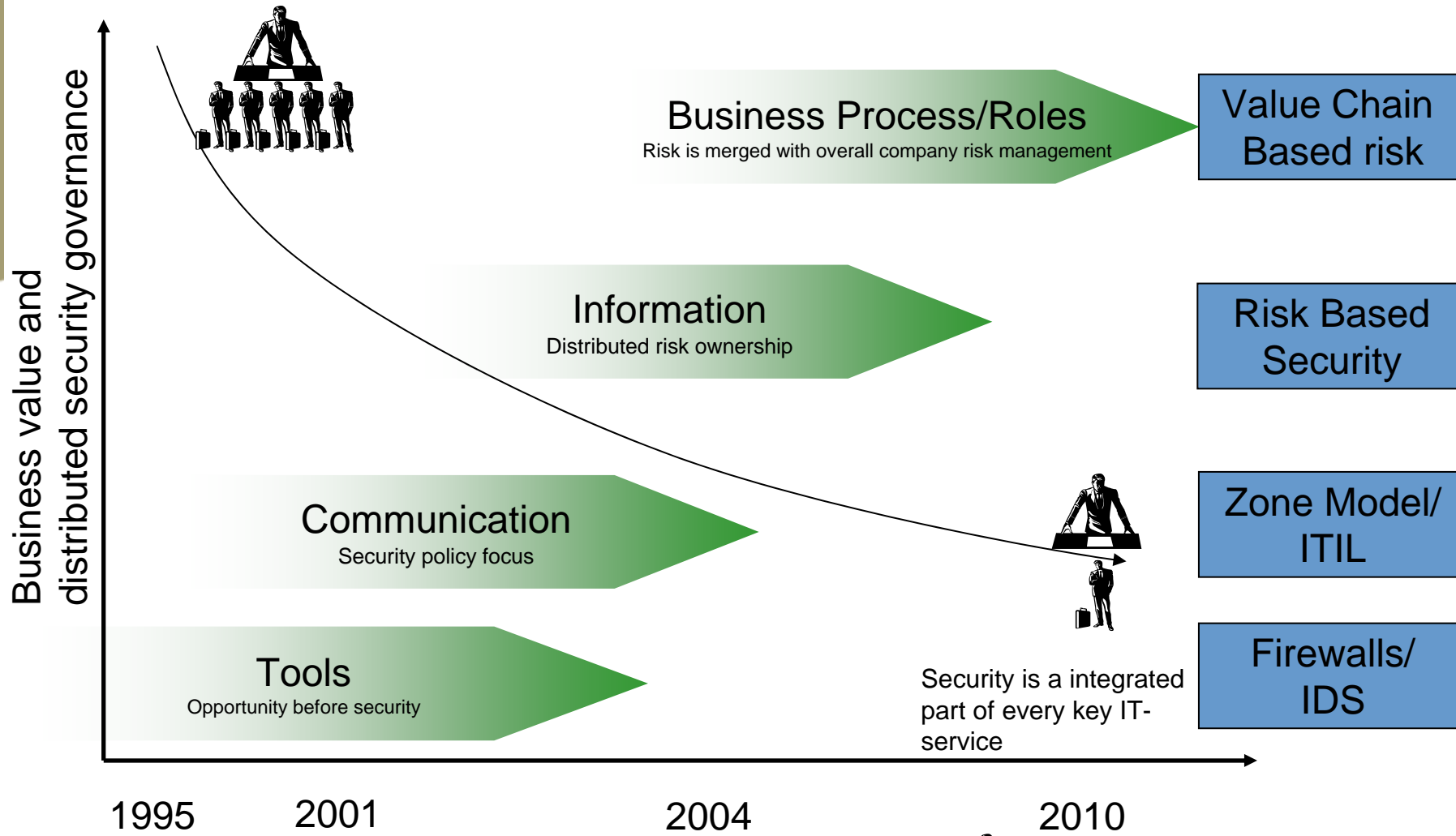


Statkraft



IT-Security Roadmap In Statkraft (2010)

Nature at work



Statkraft



IT – Framework for Security

IT security for Statkraft is:

- Know and monitor risk
- Manage risk in a manner that preserves expected risk level

Security is a combination of technique and attitude

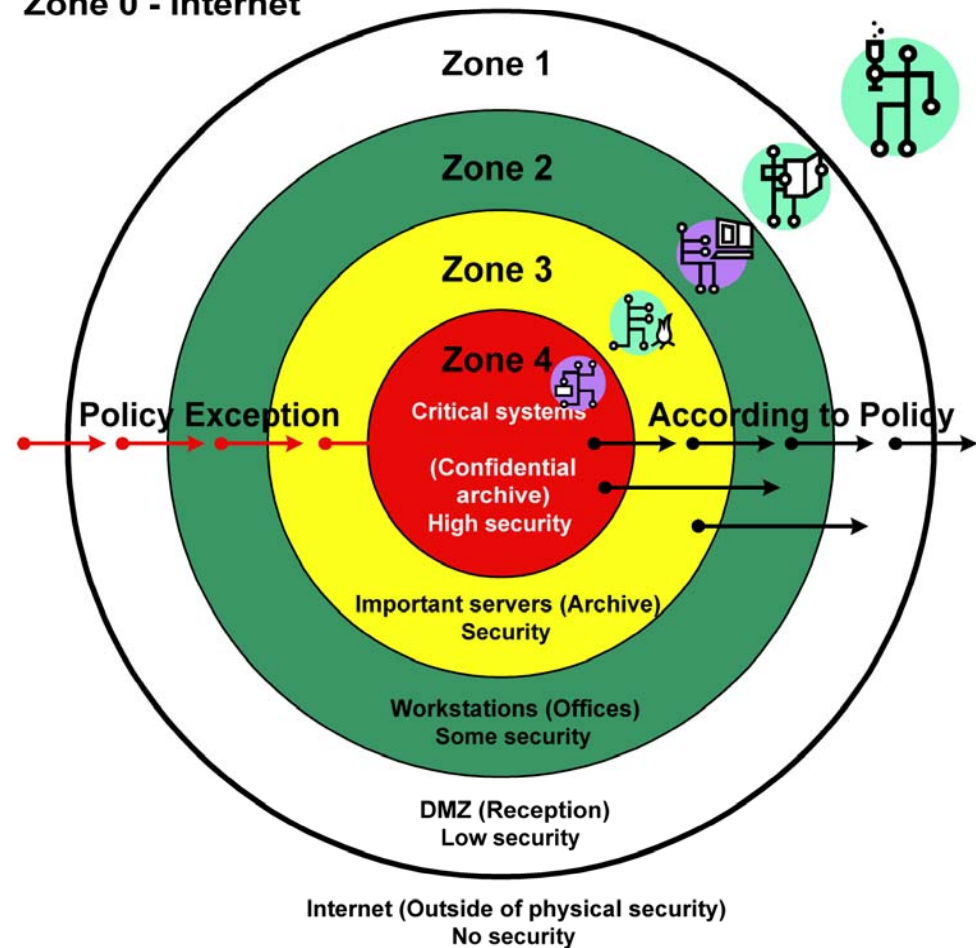
Security for Statkraft is based on 4 principles that simply communicate important IT- security issues

- Preserve Security Zone model
- KISS
- Make it Personal
- Whitelist

Allow business flexibility based upon stakeholder risk acceptance

IT security services preserve the security infrastructure

Zone 0 - Internet



*Nature
at work*



Statkraft



IT-Risk management model

Nature at work



Threats



Actions



Risk Assessment

Probability of Threats

- Loss of access
- Loss of data
- Misuse
- Error in data

Business values

- Health Environment Safety (HMS)
- Damage to reputation
- Financial loss
- Loss of business secrets
- Laws and regulations

$$\text{Probability} * \text{Consequence} = \text{Risk}$$

Owned by IT delivery

Must be owned by Stakeholder



Statkraft

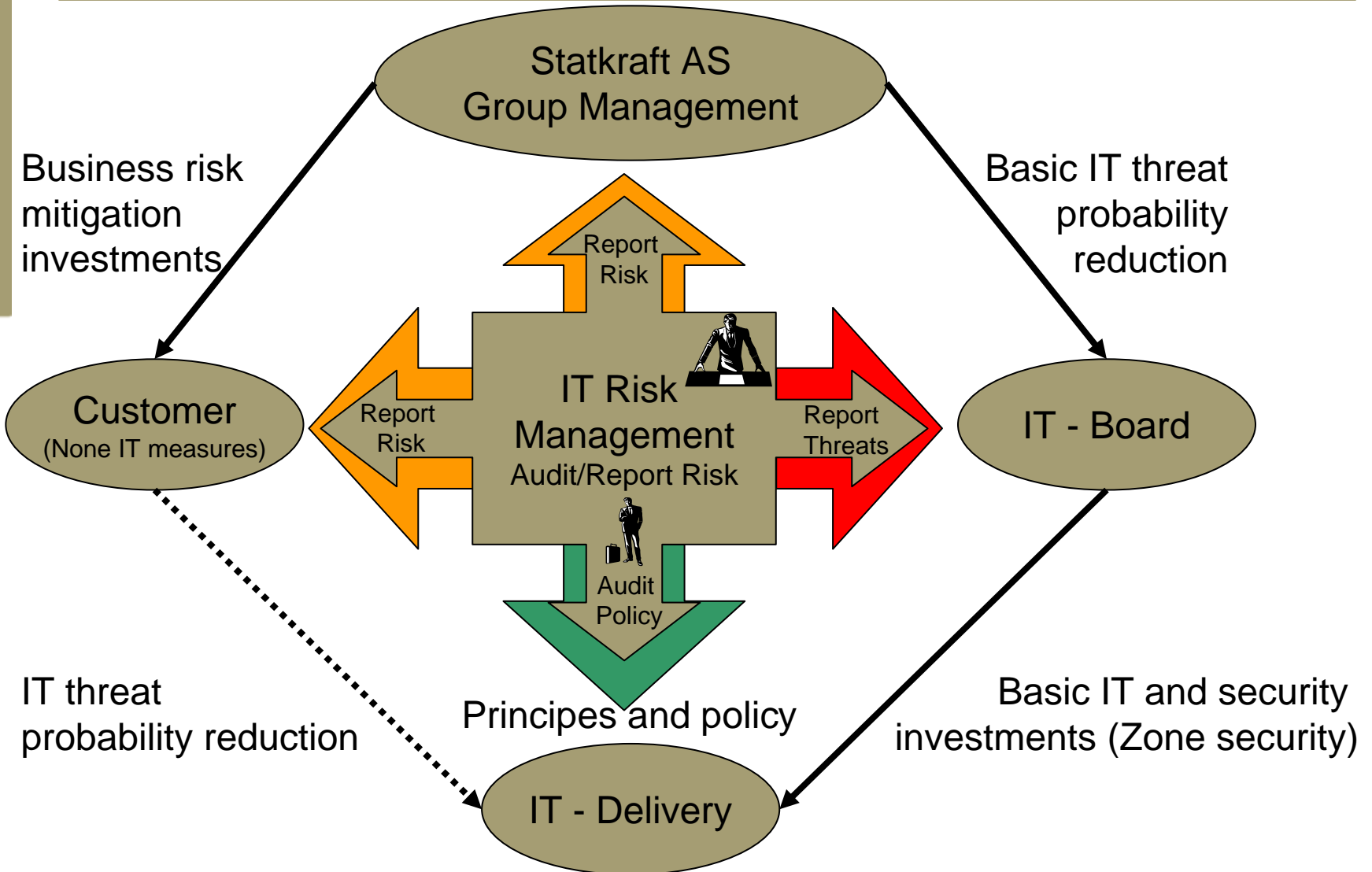


IT Risk Management company function

Nature at work



Statkraft

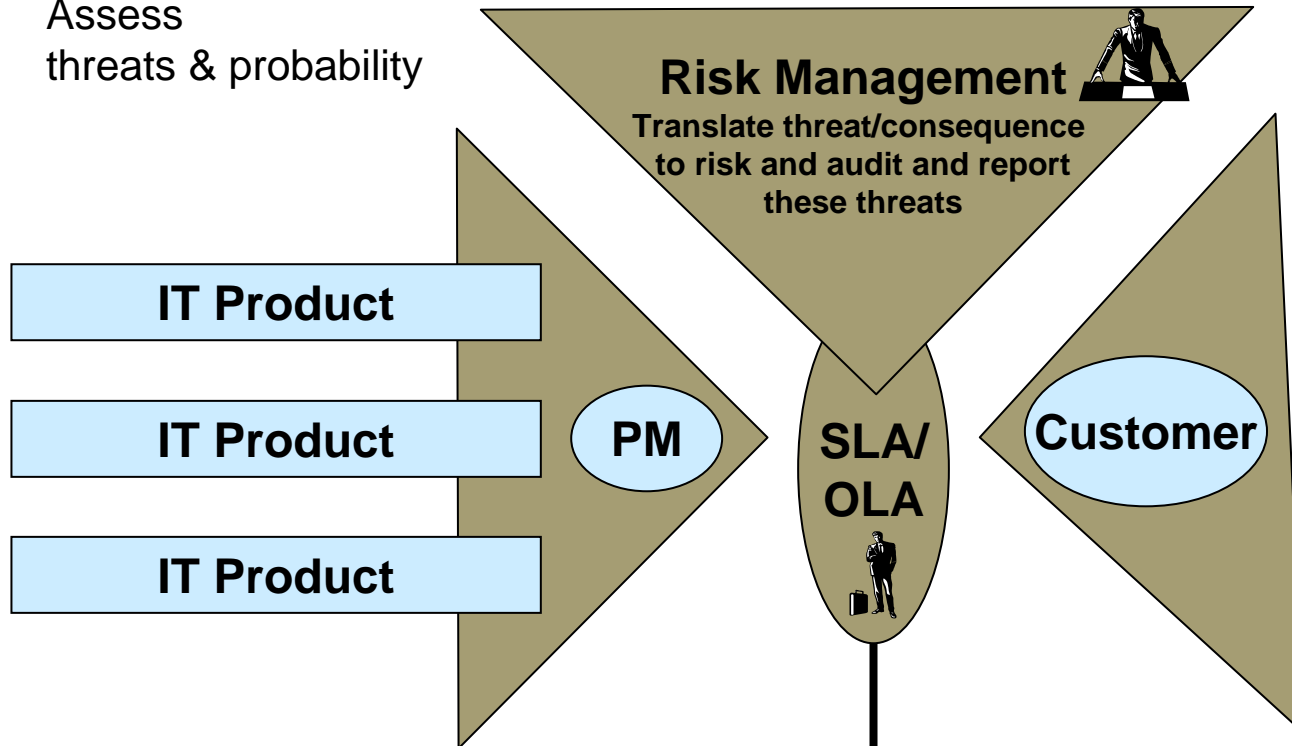




IT Risk Management services

Assess threats & probability

Assess consequence to business values



Emergency response and security responsibility is held by the product manager

Risk/consequence responsibility is with the customer

Nature at work



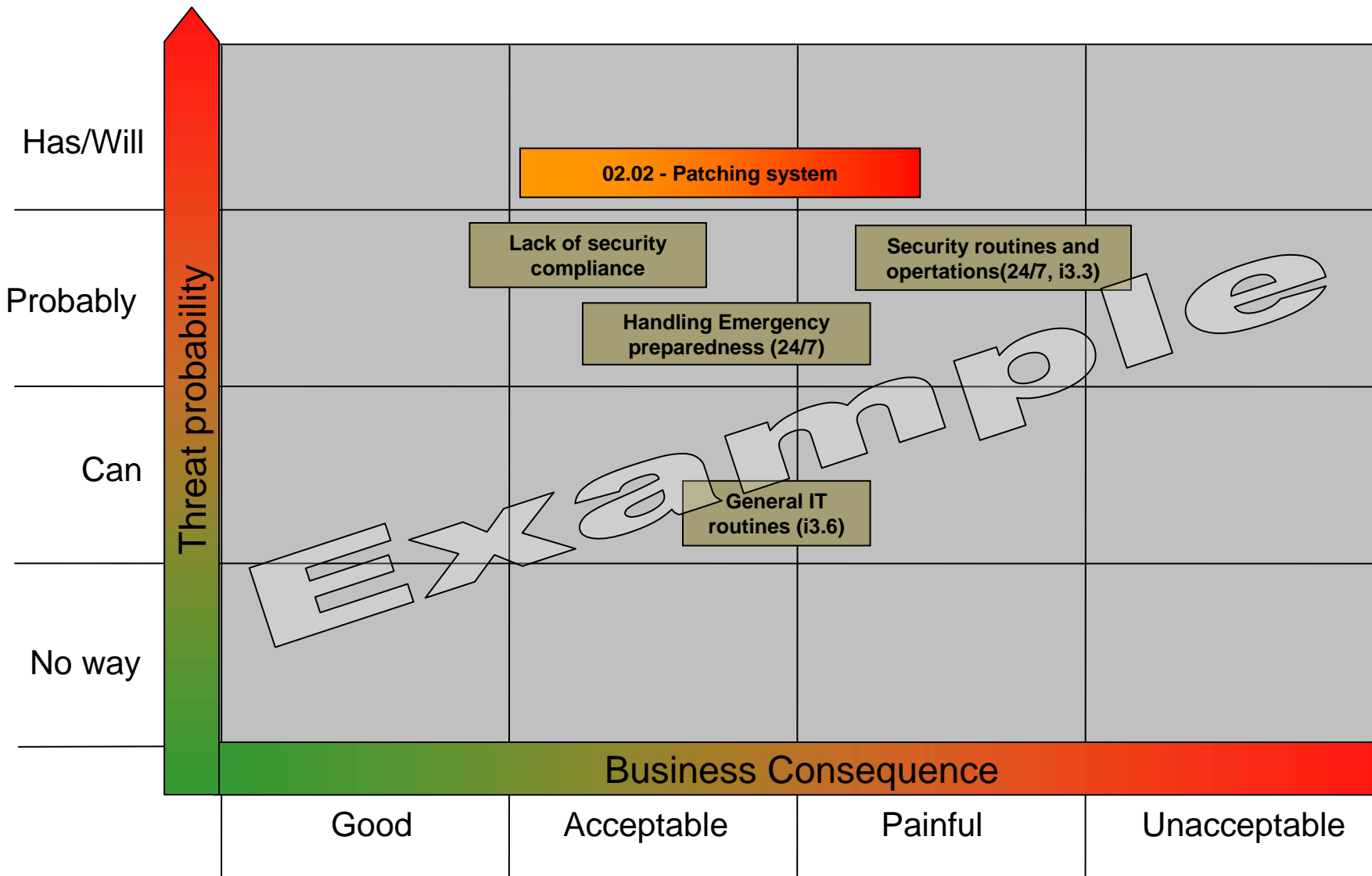
Statkraft



Statkraft – Monthly Risk Exposure

Vulnerability and incidents

Nature at work



Actual Incident
 Potential incident
 Lack of compliance to security policy



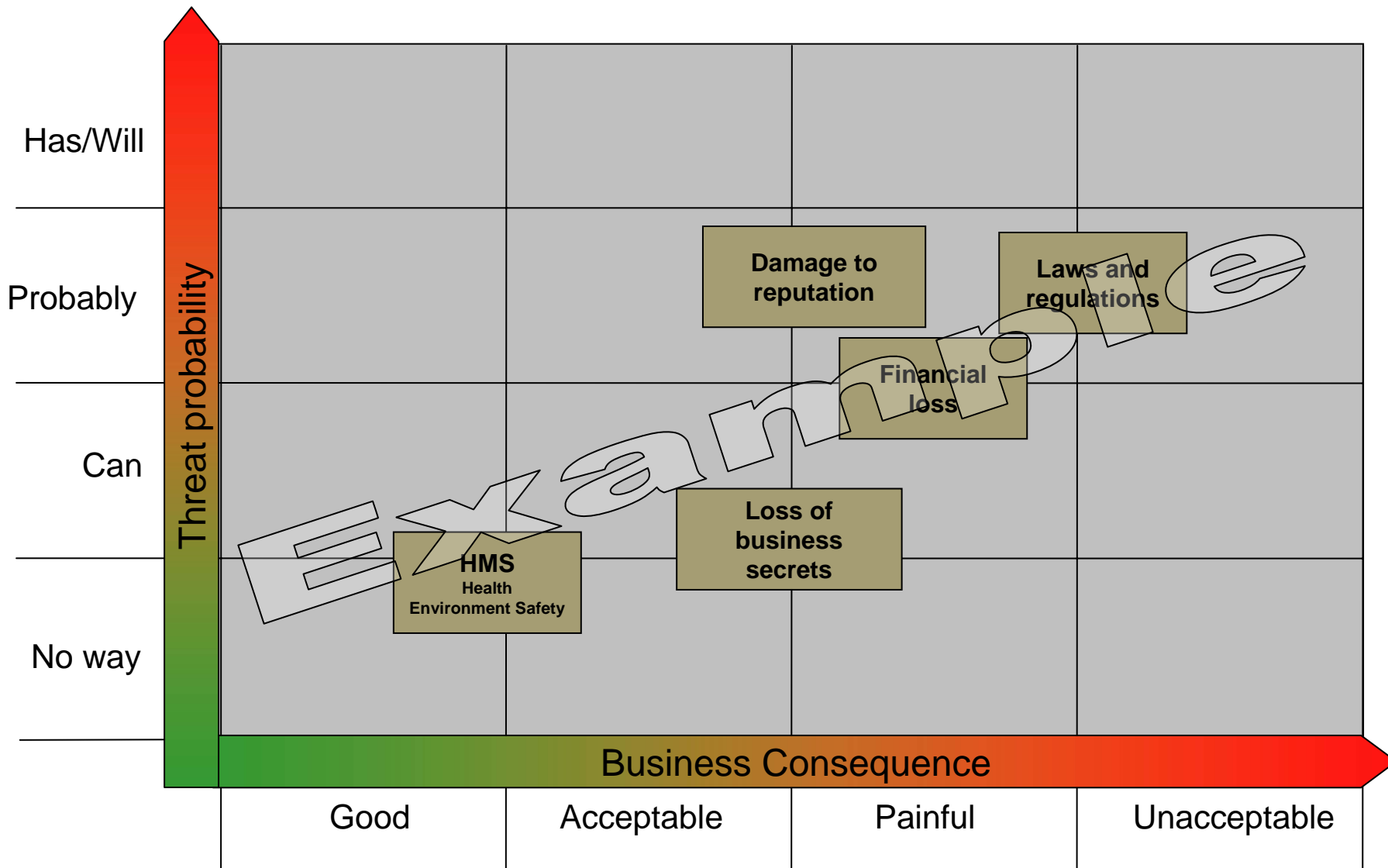
Statkraft



Statkraft – Monthly Business Risk Exposure

Compliance/vulnerability current potential loss

Nature at work



Actual Incident Potential incident Lack of compliance to security policy



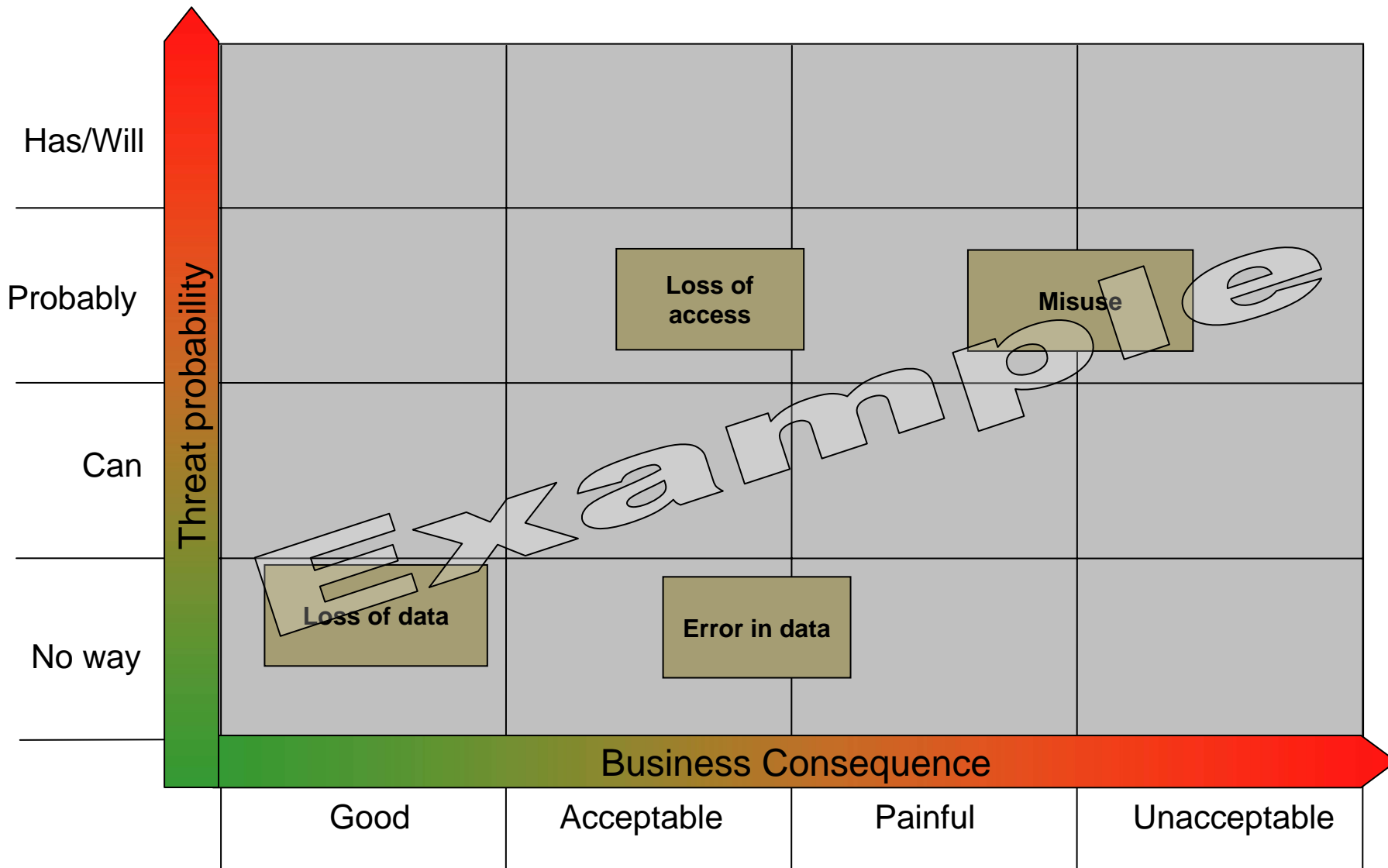
Statkraft



Statkraft – Monthly Threat assessment

Risk mitigation focus areas for risk reduction

Nature at work



Actual Incident Potential incident Lack of compliance to security policy



Statkraft



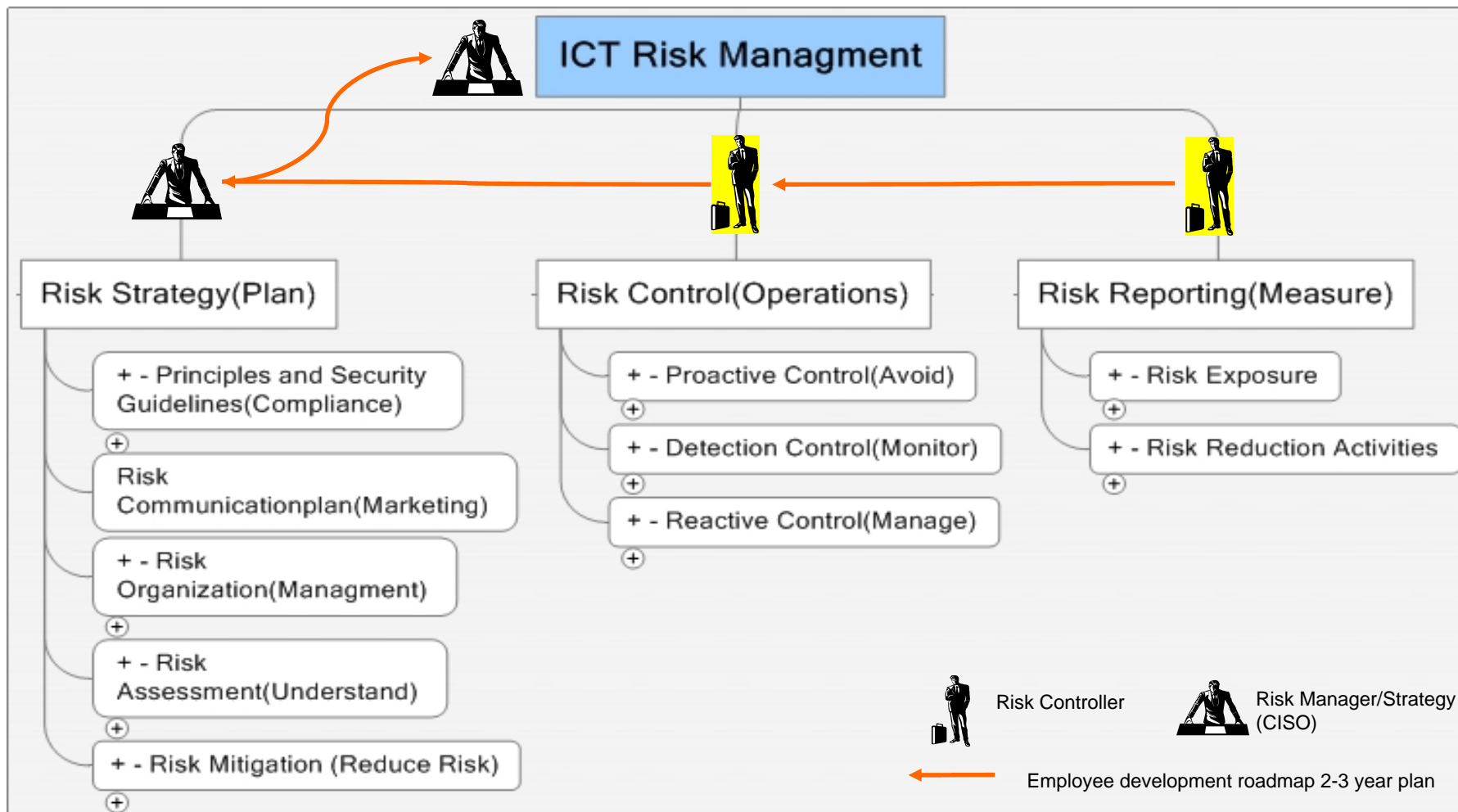
IT-Risk Management

Governance map and implementation



Overview, monitoring and managing probability of threats that can cause loss of business values

Nature at work



Statkraft

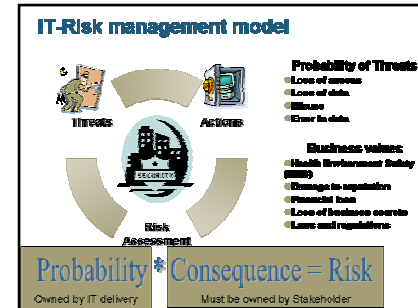


Agenda – Summery

Nature at work

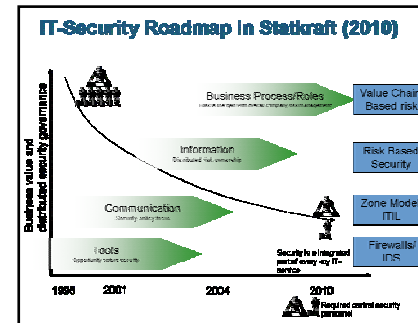
Framework

- 'Make it personal' is the reason and basis for Statkraft implementation of Risk Management



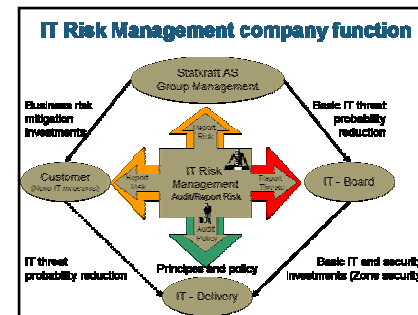
Security policy importance and function

- Security policy is reduced to standards and central security roles by introduction of risk management



Distributed security governance

- The customer takes responsibility for risk and consequence of threats caused by IT services
- IT product managers are responsible for communicating threats and their probability of occurrence



Statkraft

Thank you for the attention



Business risk consequence rating

Nature at work

Business impact	Loss of Life	Permanent loss of credibility	1 Bill	Undetected loss of confidential data	Prison	Unacceptable
	Injury	Long-term loss of credibility	100 Mill	Detected loss of confidential data	Fine	Painful
	Minor Injury	Incident quickly forgotten	1 Mill	Loss of internal data	Slap on the wrist	Acceptable
	No Injury	Not affected	100 Thousand	None	None	Good
	HMS Health Environment Safety	Damage to reputation	Financial loss	Loss of business secrets	Laws and regulations	



Statkraft



Threat rating

Nature at work

	Loss of access	Loss of data	Error in data	Misuse	
H	More then a day (uncontrolled)	Unrecoverable data	Will not be detected	Undetected full administrative access	High
M	Less then a day	Recoverable within a week	May be detected	External detected/ traceable access	Medium
S	Less then an hour	Recoverable within a day	Will be detected	Internal detected	Low
L	Less then 10 minutes	Recoverable within an hour	Will be detected and can be corrected	Internal detected/ traceable access	
Threat can not occur					None



Statkraft



Risk model: HMS Example risk assessment

Nature
at work

	Business Consequence			
	Good	Acceptable	Painful	Unacceptable
	No Injury	Minor Injury	Injury	Loss of Life
Loss of access	L S	M H		
Loss of data	L	S	M	H
Error in data	L S	M H		
Misuse	L	S M		H

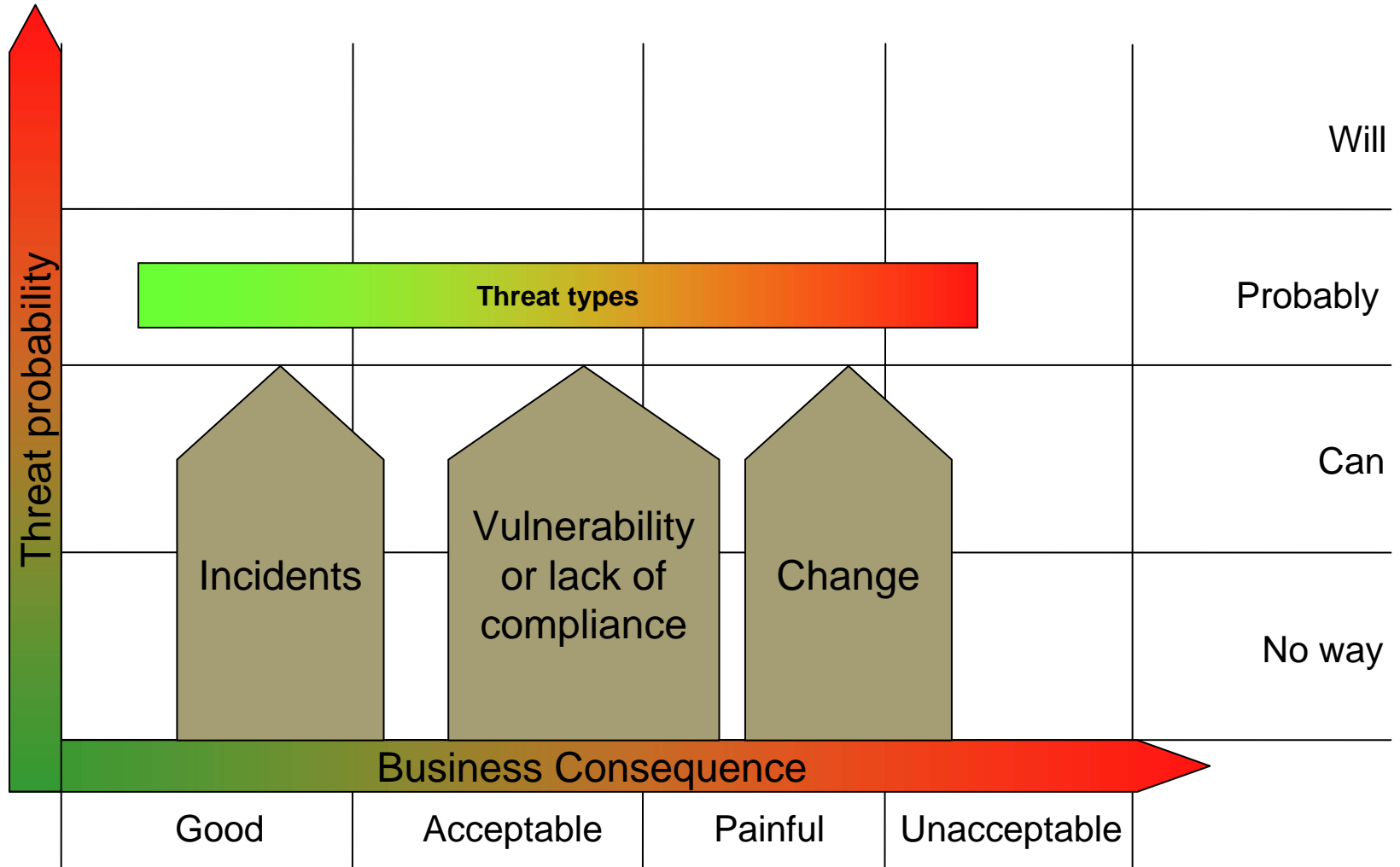


Statkraft



The three areas that can or has caused security incidents

Nature at work



Statkraft