Nature at work

Statkraft

IT-Security policy and Risk Management

IT-Security IS Risk Management

Agenda – What will this session cover

Framework

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

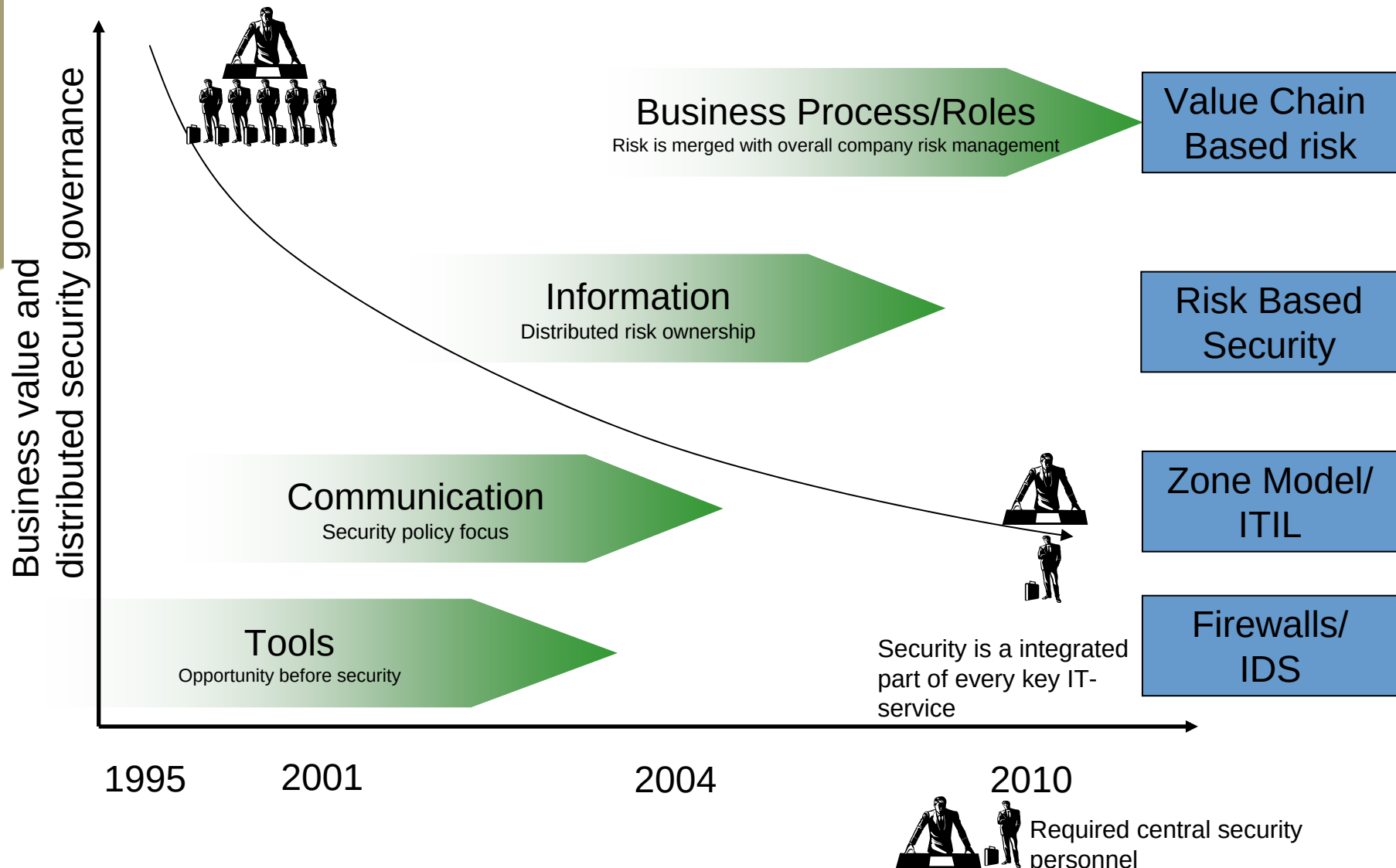
Security policy importance and function

- 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

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**

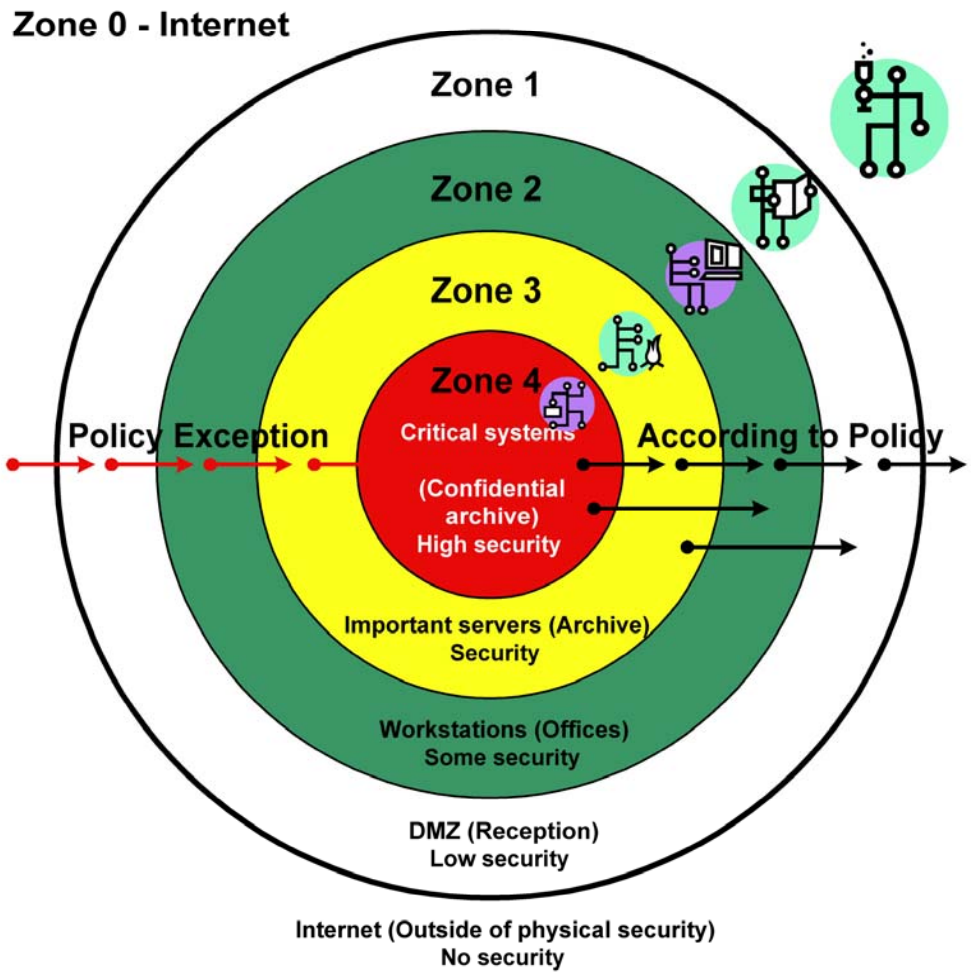
Security is a combination of technique and attitude

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



Nature at work

Statkraft

IT-Risk management model

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

Probability * **Consequence = Risk**

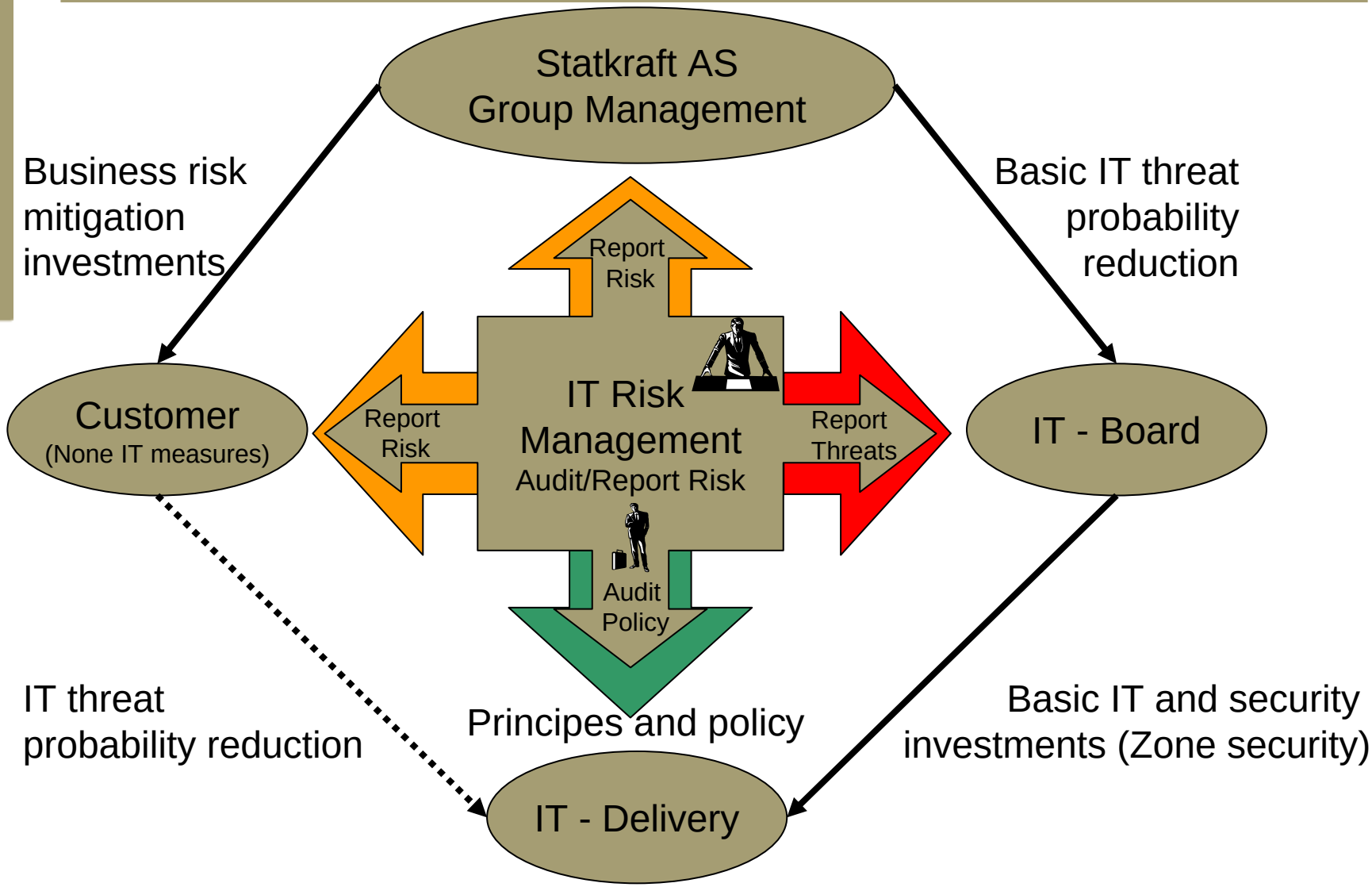
Owned by IT delivery

Must be owned by Stakeholder

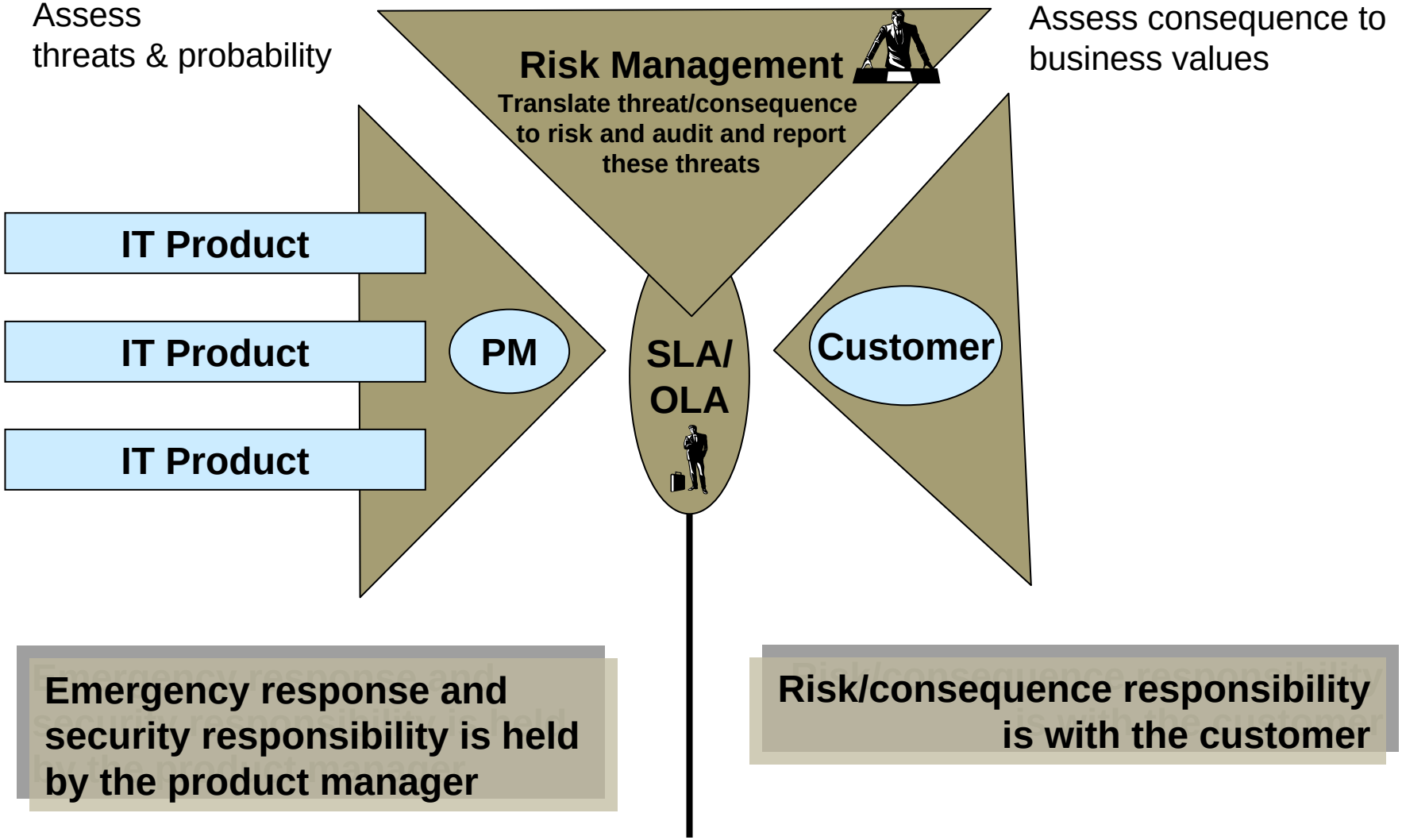
Nature at work

Statkraft

IT Risk Management company function



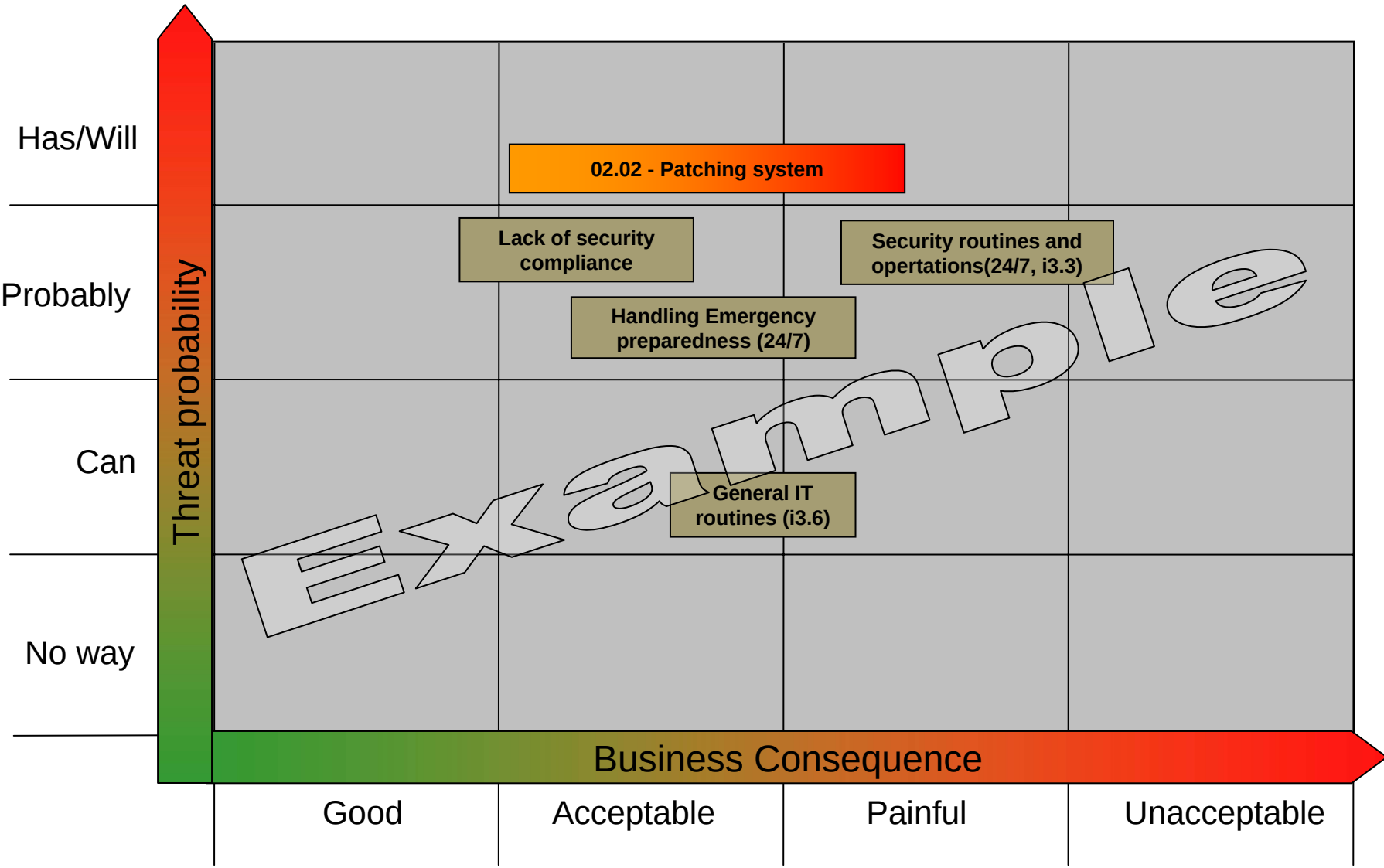
IT Risk Management services



PM: Product manager (Norwegian: Leveranse ansvarlig)

Statkraft – Monthly Risk Exposure

Vulnerability and incidents

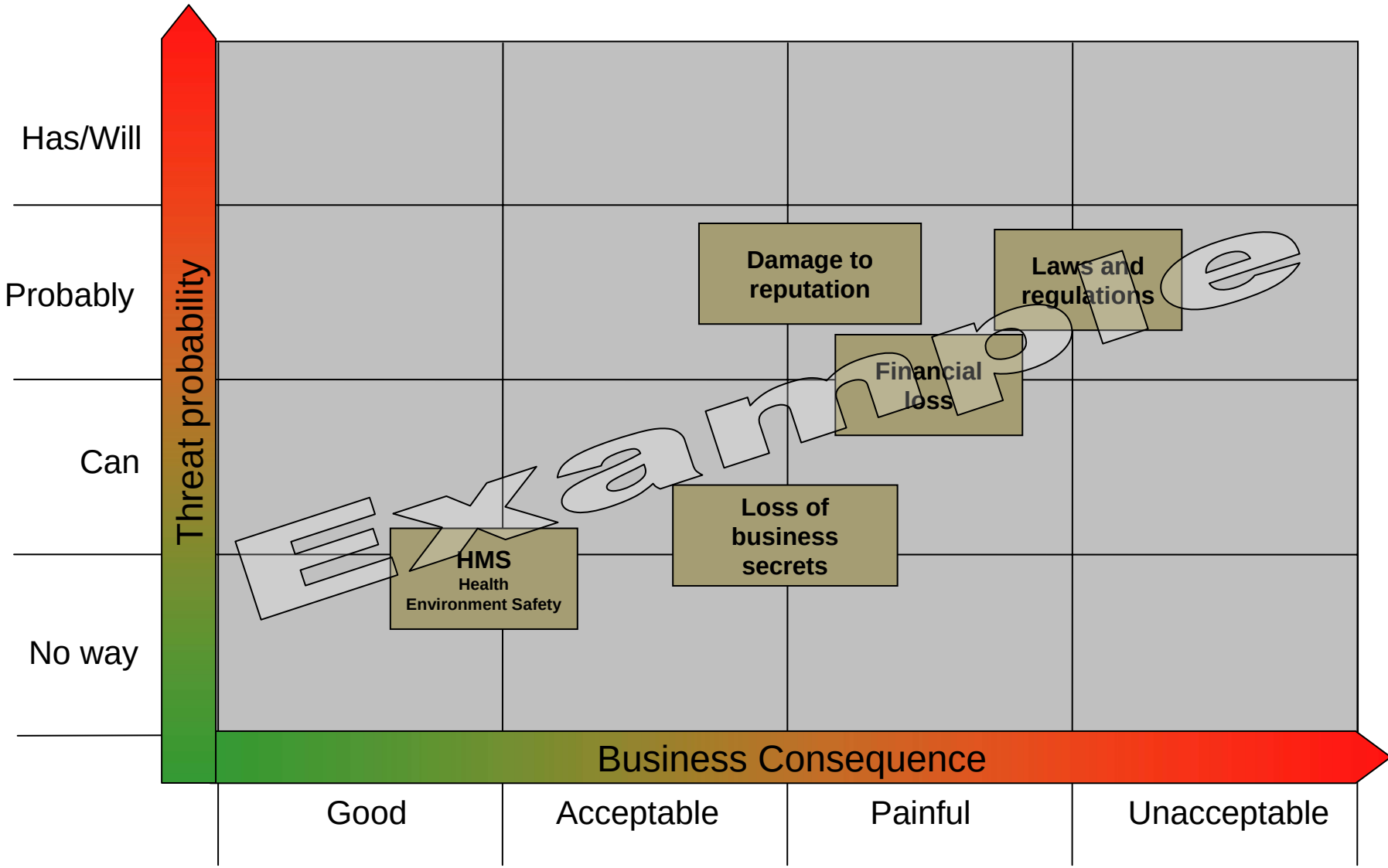


Nature at work

Statkraft

Statkraft – Monthly Business Risk Exposure

Compliance/vulnerability current potential loss



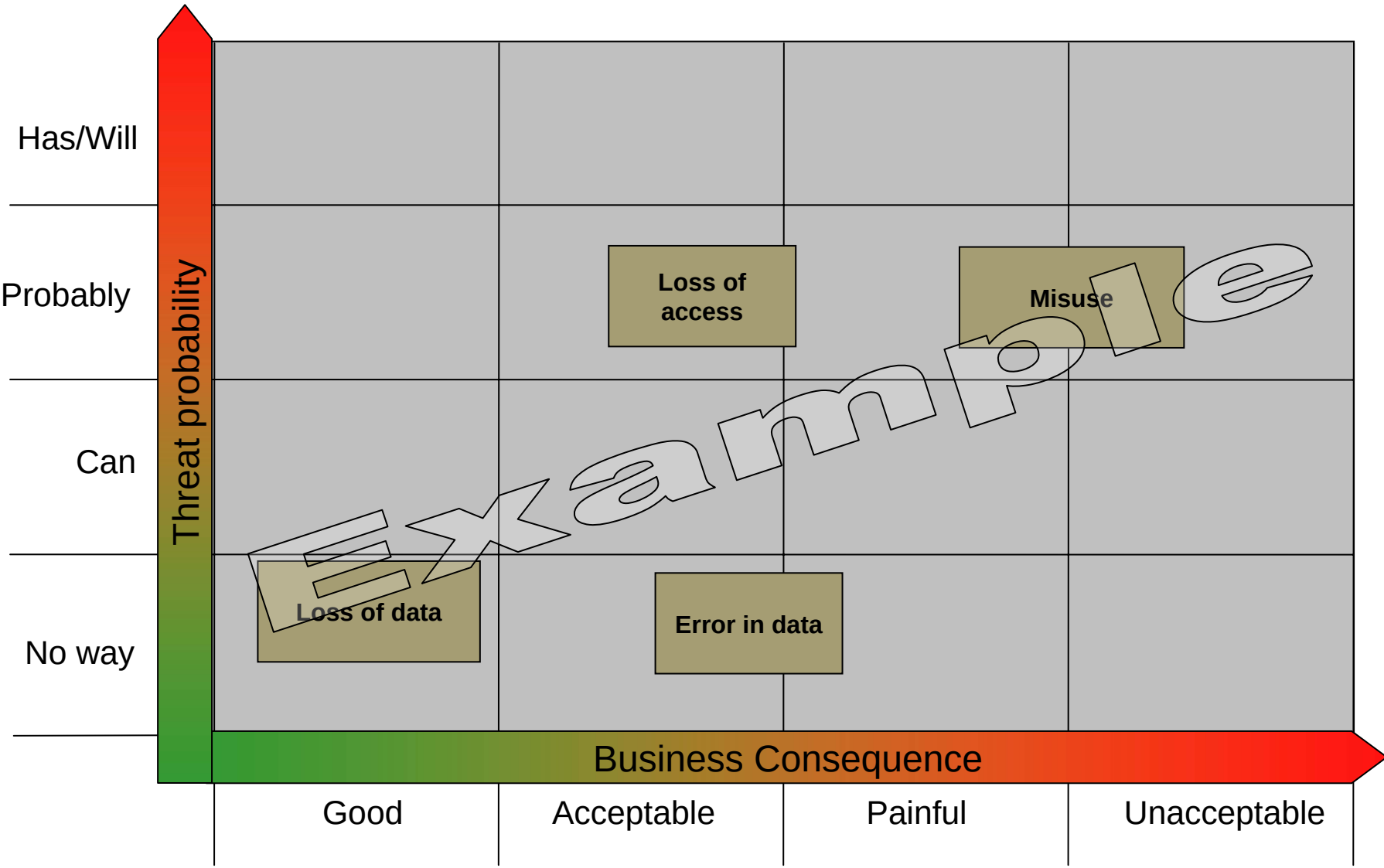
Actual Incident | Potential incident | Lack of compliance to security policy

Nature at work

Statkraft

Statkraft – Monthly Threat assessment

Risk mitigation focus areas for risk reduction



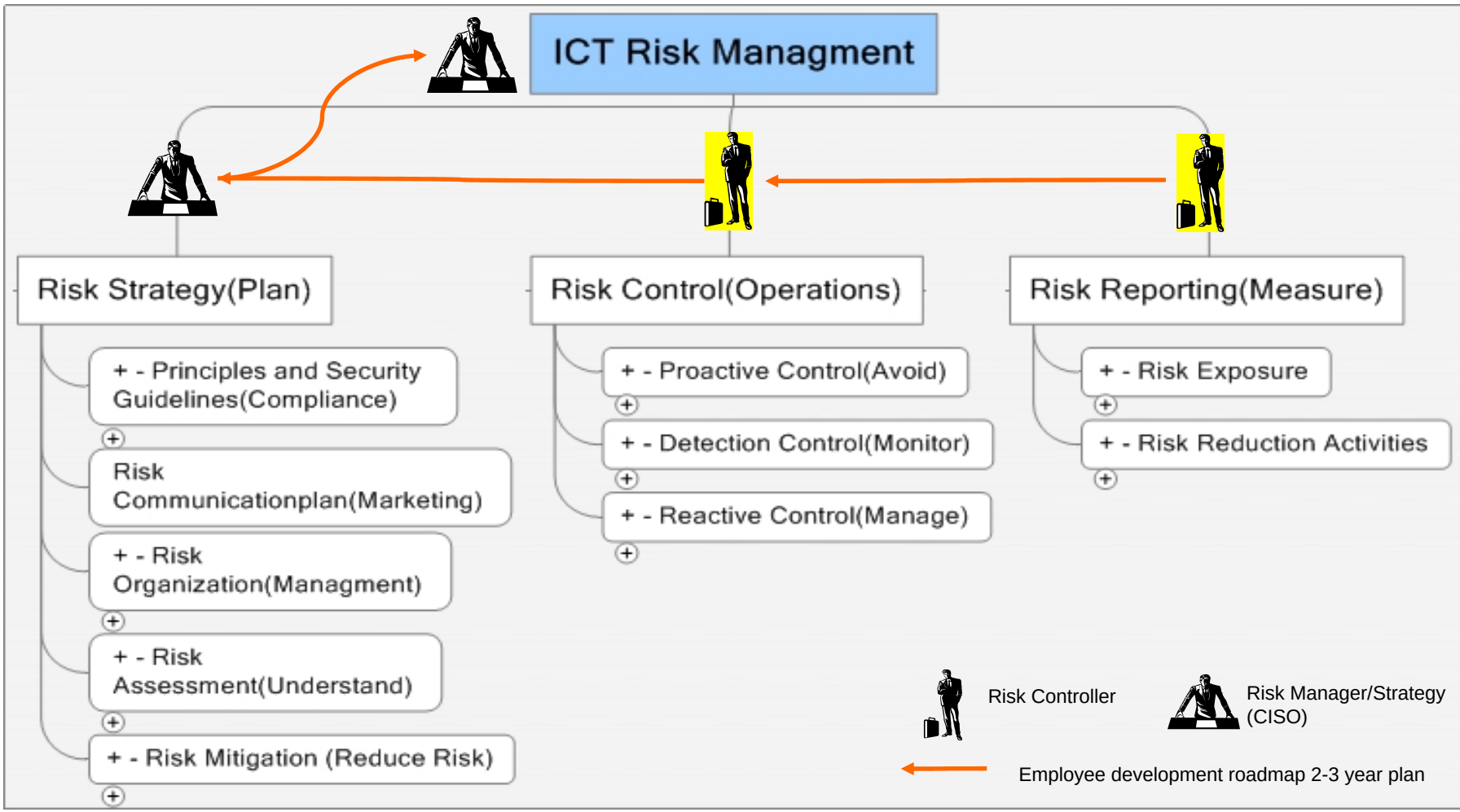
Nature at work

Statkraft

IT–Risk Management

Governance map and implementation

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



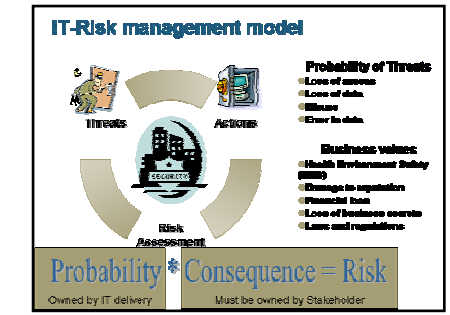
Nature at work

Statkraft

Agenda – Summery

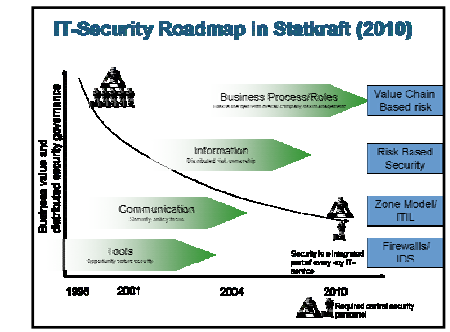
Framework

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



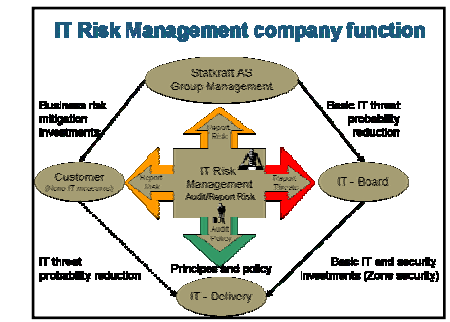
Security policy importance and function

- 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



Thank you for the attention

Business risk consequence rating

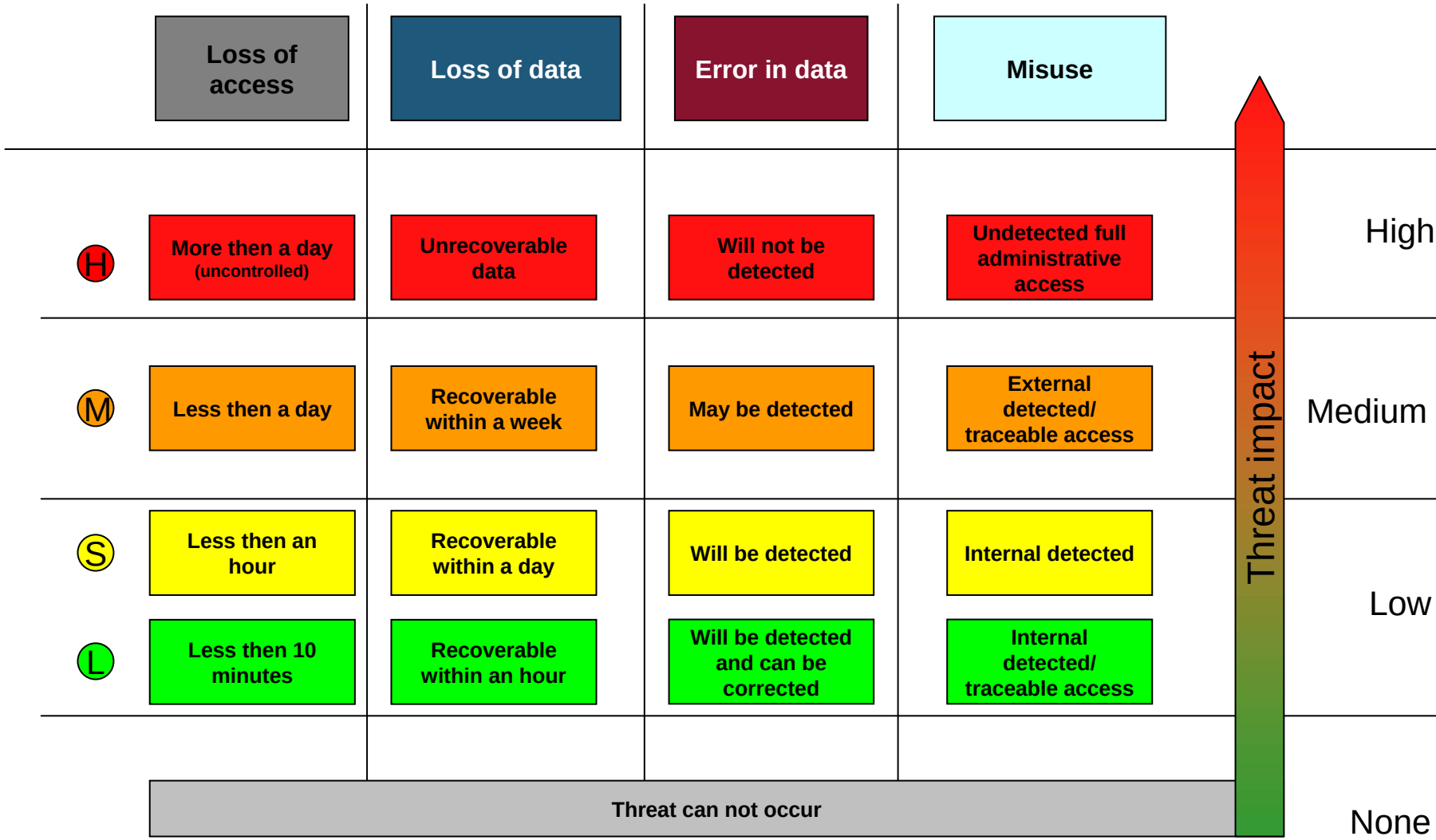
Business impact

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

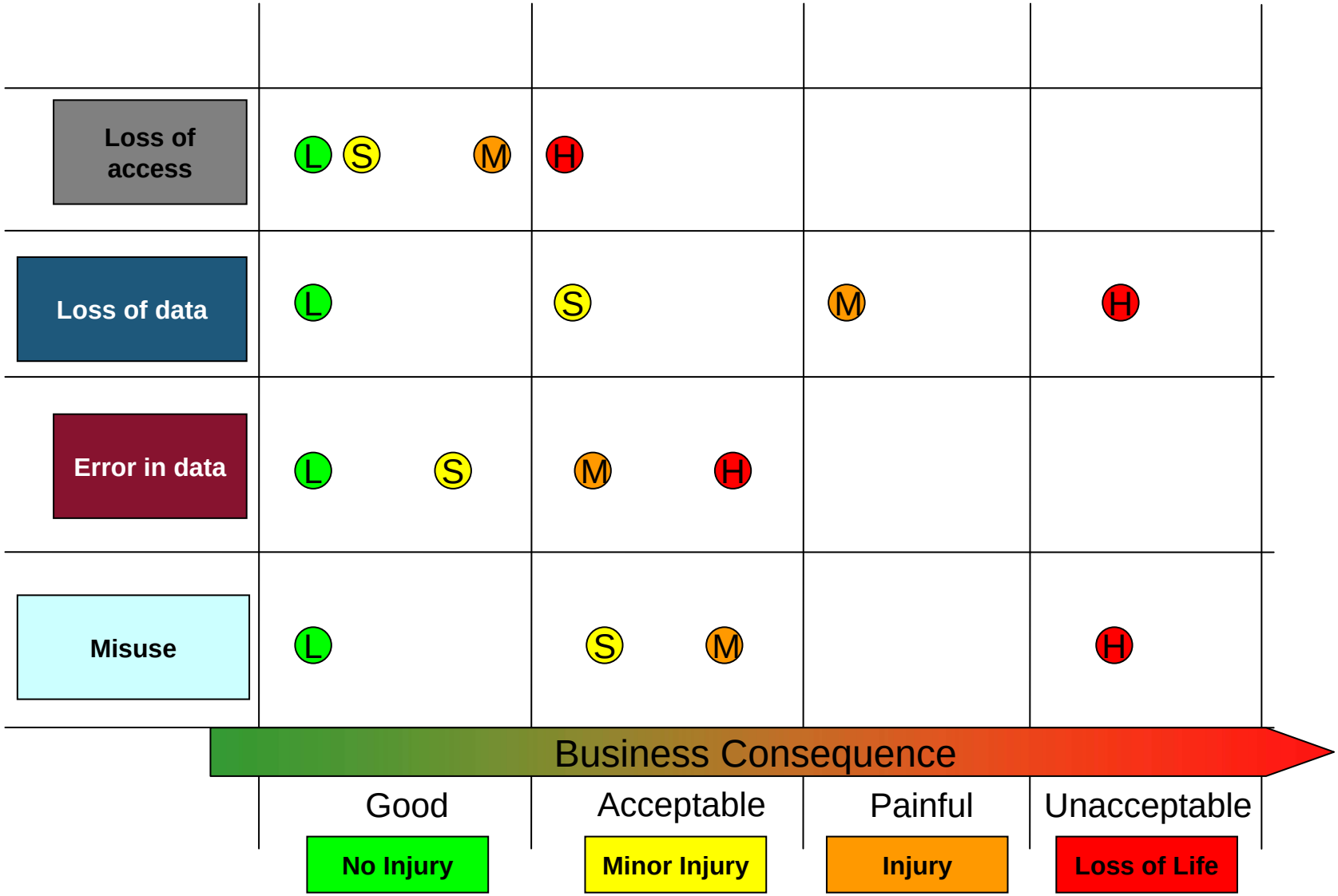
Nature at work

Statkraft

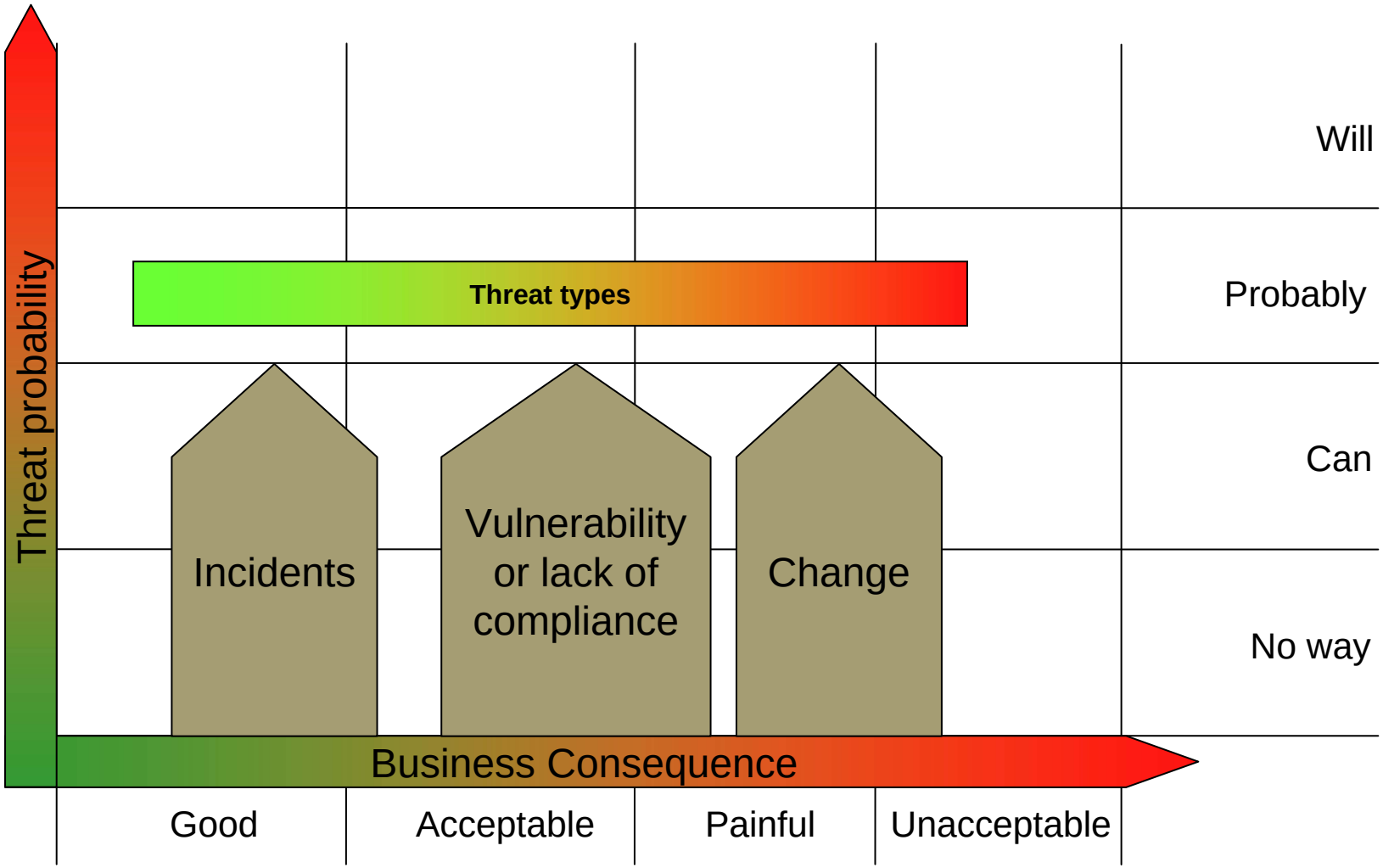
Threat rating



Risk model: HMS Example risk assessment



The three areas that can or has caused security incidents



Nature at work

Statkraft