SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

# ROS analyse for samfunnskritiske IKT systemer

## Utfordringer og muligheter

24/11-05

Hermann Steen Wiencke
Proactima/Universitetet i Stavanger

proactima
PRO-ACTIVE MANAGEMENT

# SEROS

**Et samarbeid mellom**
**Universitetet i Stavanger og Rogalandsforskning**

**Ta kontakt med oss på:**
**www.seros.no**

# Presentasjon

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

- Bakgrunn for BAS 5 prosjektet
- Utvikling av ROS metodikk
- Erfaringer: utfordringer og muligheter

proactima
PRO-ACTIVE MANAGEMENT

# BAS 5 prosjektet

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

## Formål

- Redusere sårbarheten av samfunnskritisk IKT, dvs. gjøre IKT systemene mer robuste mot ulike trusler, villede handlinger og ulykker.

- Finne frem til tiltak som kan redusere sårbarheten av IKT systemene
  - Tekniske tiltak
  - Organisasjon
  - Arbeidsprosesser
  - Regelverk og krav
  - …….
- Prioritere tiltakene, slik at man starter med de viktigste systemene og de mest effektive tiltakene.

- Påvirke design og utbygging av nye systemer.

proactima
PRO-ACTIVE MANAGEMENT

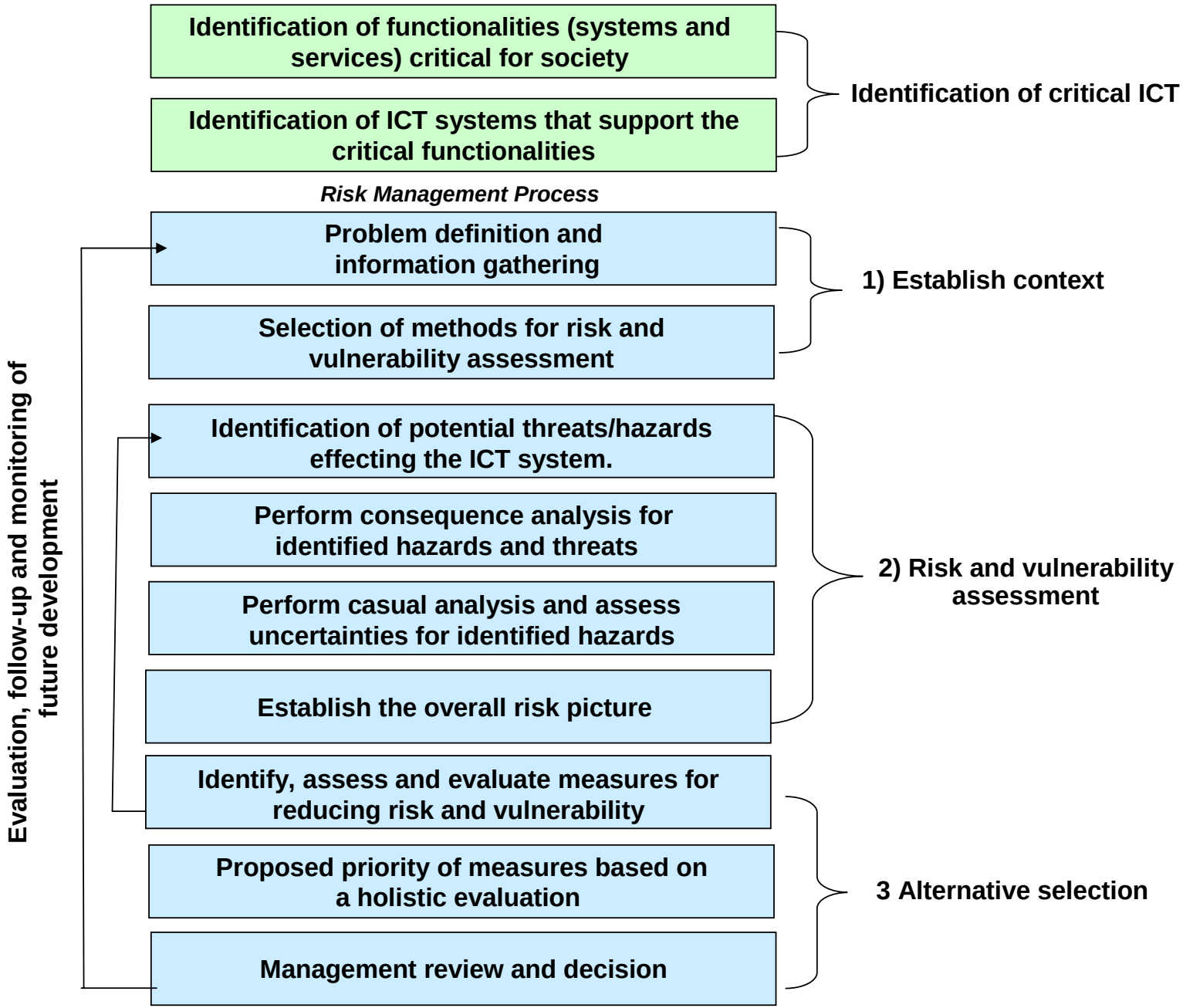
# BAS 5 - Fremgangsmåte

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET

- Vurdering av etablert praksis/litteraturstudie.
- Etablert en risiko og sårbarhets analyseprosess som reflekterer helheten i BSA 5 prosjektet
- Etablere et rammeverk for valg av riktig metode:
  - **Vurdering av etablerte metoder og teknikker**
  - **Gjennomgang av Case med bruk av utvalgte metoder**
- Test av rammeverket – klassifisering av problemstilling og valg av metode. (ikke komplette case)
- Oppdatering/forbedring av metode og rammeverk.

proactima
PRO-ACTIVE MANAGEMENT

# Helhetlig fremgangsmåte



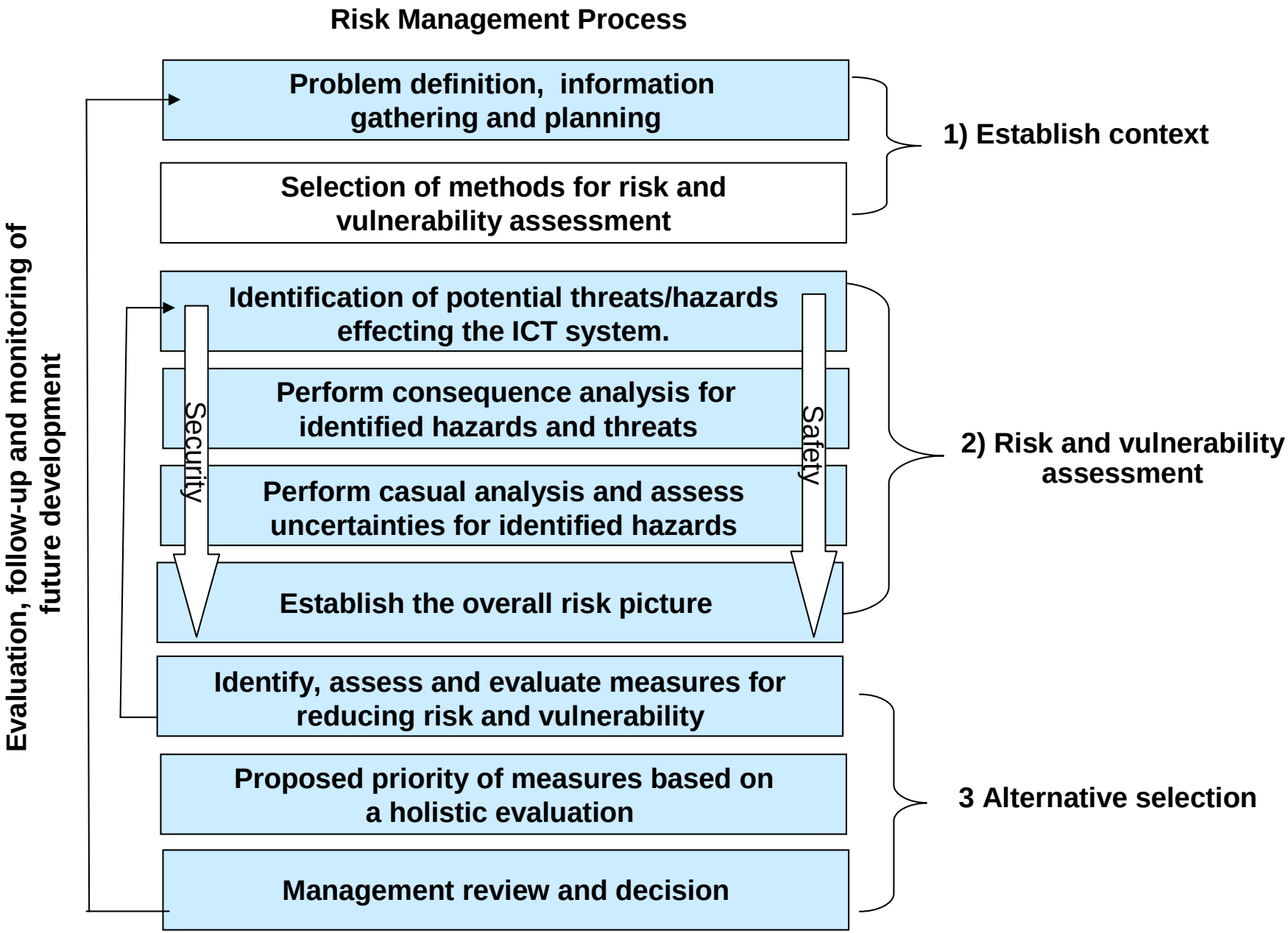
# Fokus område

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

- Basis for BAS 5 er en generell risikostyrings prosess

- Fokus vil være på de områdene der BAS 5 kan bidra til ny innsikt og kunnskap og forbedre risikostyringsprosessen. To hovedområder:
  - Et rammeverk for valg av metode for risiko og sårbarhetsanalyser
  - En helhetlig tilnærming som omfatter både sikkerhet og security.

proactima
PRO-ACTIVE MANAGEMENT


Risk Management Process
Problem definition, information gathering and planning
Selection of methods for risk and vulnerability assessment
1) Establish context
Identification of potential threats/hazards effecting the ICT system.
Perform consequence analysis for identified hazards and threats
Perform casual analysis and assess uncertainties for identified hazards
Establish the overall risk picture
Security
Safety
2) Risk and vulnerability assessment
Identify, assess and evaluate measures for reducing risk and vulnerability
Proposed priority of measures based on a holistic evaluation
Management review and decision
3 Alternative selection
Evaluation, follow-up and monitoring of future development

# Etablere Rammeverk

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

## Krav til rammeverket:

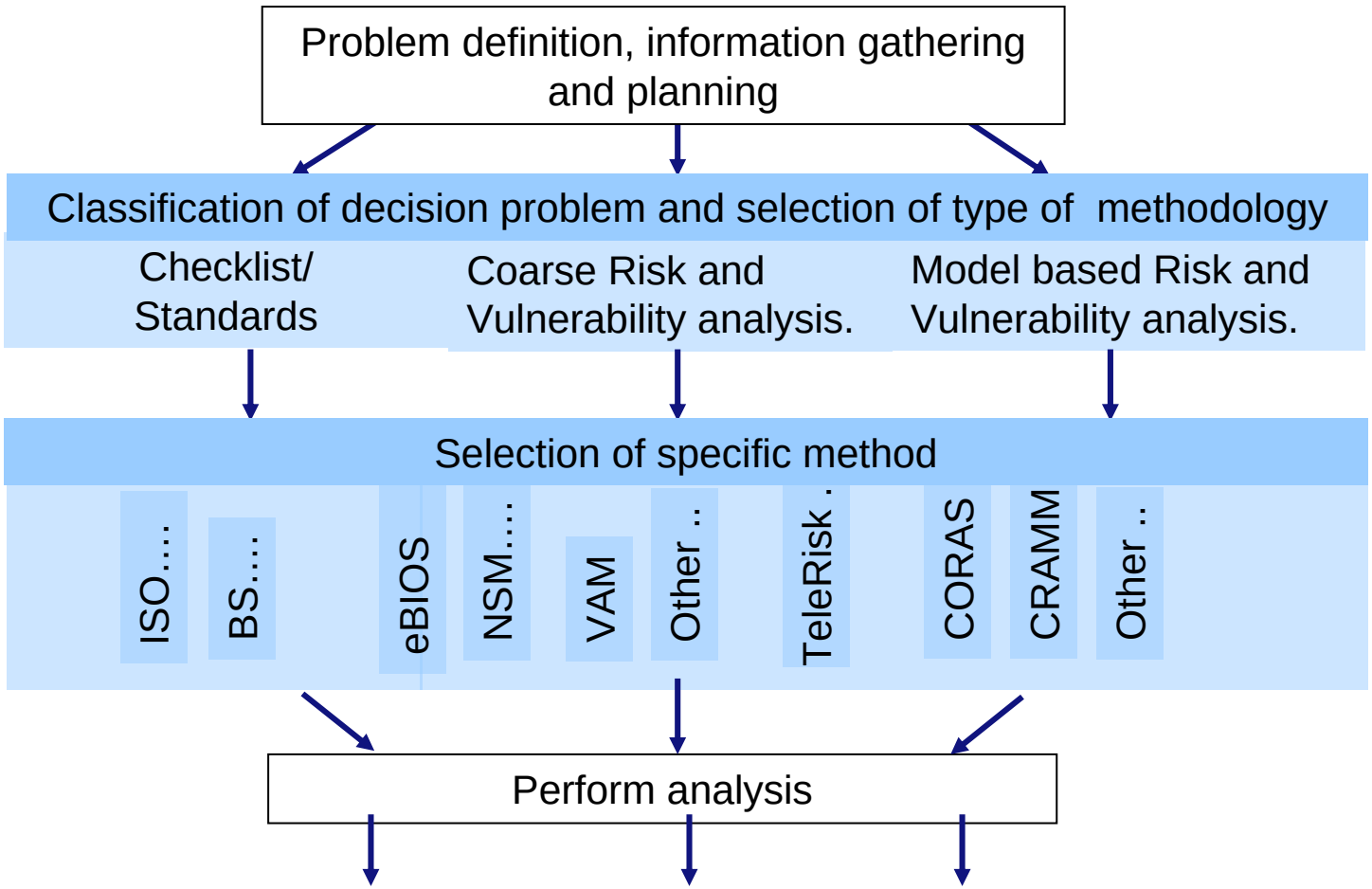
- Effektive og målrettet prosess
  - Gir ønskede resultater
  - Fornuftig ressursbruk
  - Enkel å bruke
  - Ikke papir eksersis

- Utnytter eksisterende kunnskap

proactima
PRO-ACTIVE MANAGEMENT

# Klassifisering og valg av metode

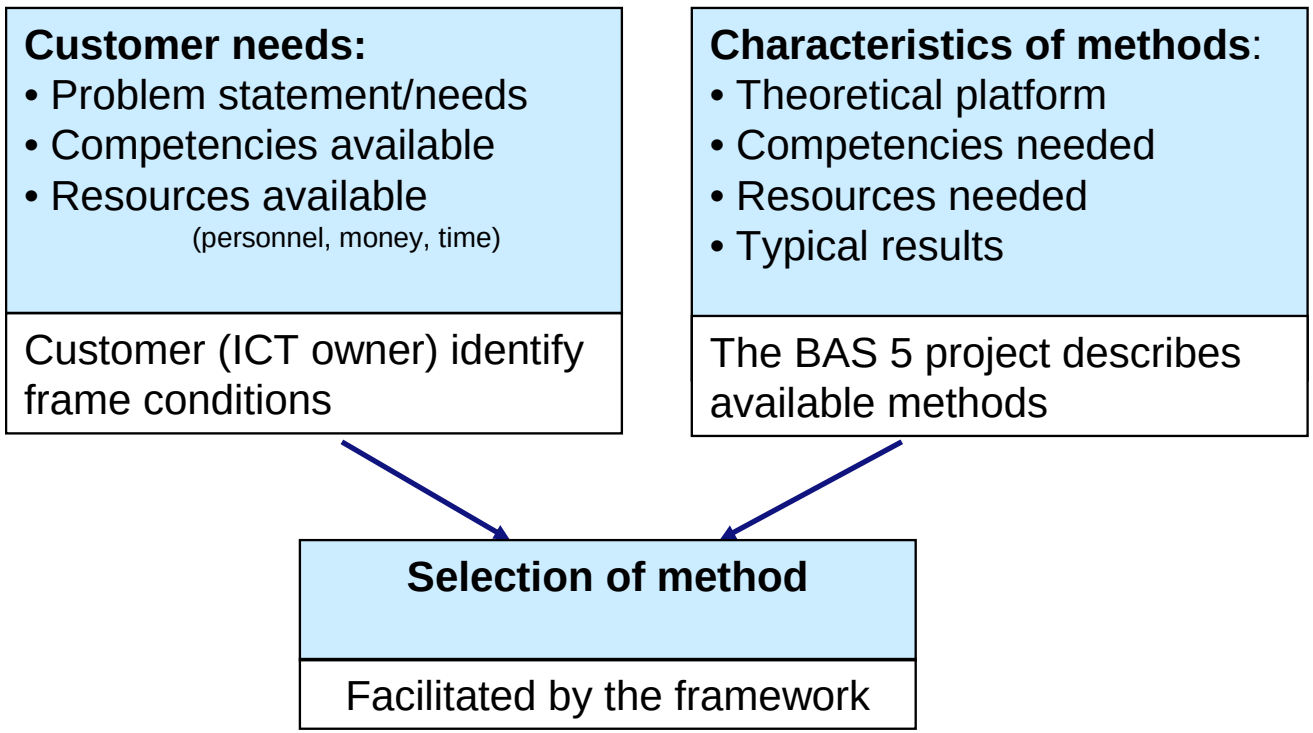
SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET




proactima
PRO-ACTIVE MANAGEMENT

# Prinsipper for valg av metode

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET




proactima
PRO-ACTIVE MANAGEMENT

# Prinsipper for valg av metode

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET

**Hva skal vi bruke resultatene til:**
-Prioritere tiltak
-Komme frem til risikotall
-Tilfredsstille lover og regler

**Hva karakteriserer systemet:**
-Komplekst (teknologi/organisasjon)
-Noe nytt/uten erfaringser
-Standard system/ har mye erfaring
-Oversiktlig
-Styrbarhet

**Hva har vi av ressurser:**
-Kompetanse
-Penger
-Tid

**Hva er sannsyneligheten for at det feiler:**
- Sannsyneligheten for et angrep
- Sårbarheten i forhold til naturhendelser
- Sårbarheten i forhold til menneskelige feil

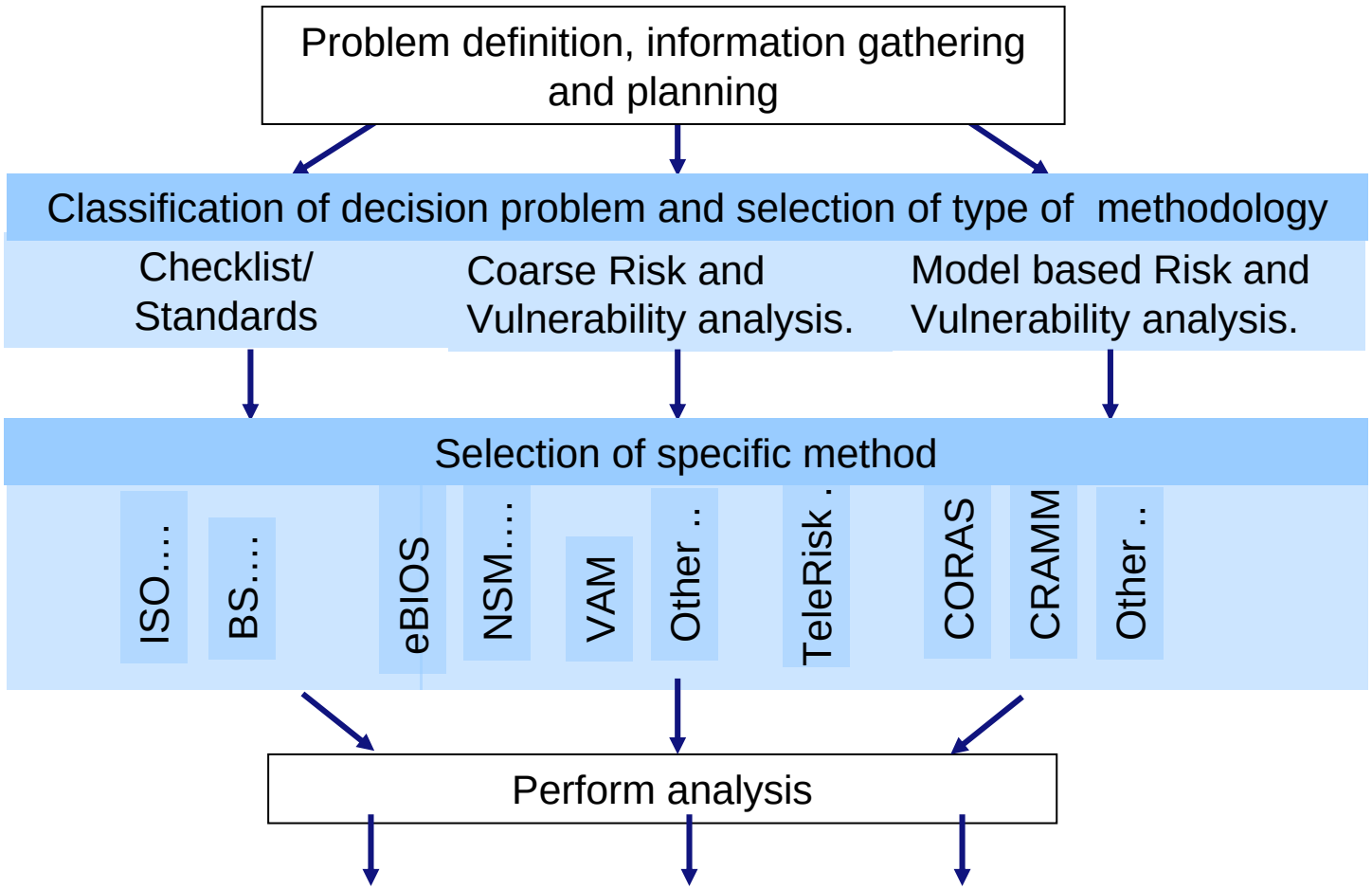
**Hva er konsekvensen av at det feiler:**
- Effekt i forhold til HMS
- Effekt for velferd
- Effekt på produksjon
- Effekt på økonomi
- Effekt for …….

**Hva forventer vi at tiltak koster:**
-Enkle tiltak
-Store investeringer
-…..

**Ikke en detaljert analyse men en klassifisering av problemstilling for å velge metode.**

# Klassifisering og valg av metode

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET




proactima
PRO-ACTIVE MANAGEMENT

# Sammendragstabell- etablerte metoder

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET

| | Framing | Planning | Identification of hazards threats | | Consequence analysis | Cause analysis and uncertainties | | Establish risk picture | Identify measures | Evaluate mesures | Priority of measures | Managerial review and decision | Comments | Recommended Application |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| METHODS | | | Safety | Security | | Safety | Security | | | | | | | |
| VAM | N | N | N | Checklist | N | N | N | N | Checklist | N | N | N | | Detailed tool for identification of vulnerabilities and measures |
| CORAS | Checklist | Checklist | Brain storming | Brain storming | Model based | | | | | | | | | |
| TeleRisk | Questioner | Questioner | Brain storming | Brain storming | Expert judgment/ model based | | | | | | | | | |
| CRAMM | | | | | | | | | | | | | | |
| NSM | N | N | Brain storming | Brain storming | | | | | | | | | | |
| EBIOS | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Detailed evaluation form**

**established for each method/tool**

N=not addressed

proactima
PRO-ACTIVE MANAGEMENT

| Risk management process | Main activities | Important issues | Requirements | To be filed in for each method: Method = xxxxx |
|---|---|---|---|---|
| | | | | |
| **Establish context** | Problem definition: Description of goals for the assessment | The background for the assessment? (poor performance, threats, regulation,…)<br>-Use of results<br>-Decisions supported | Process for problem definition and establishing goals | |
| | Identify relevant concerns, functions, performance measures and possible decision criteria System definition | -Relevant concerns (political, ethical, precautionary, use of new technology, etc.)<br>-Functions e.g. delivery of electrical power<br>-Performance measures: damage levels, number of fatalities, quantities related to confidentiality, integrity, etc.)<br>-Safety / security<br>-ALARP processes<br>-Risk acceptance criteria<br>-Other requirements | -Process for identifying relevant concerns, functions, performance measures and decision criteria | |
| | Establish project team and establish project plan | -Budget<br>-Schedule<br>-Selection of methodology<br>Competencies<br>-Risk analysis<br>-Business/domain | - Tools for facilitation of the planning process<br>- Method for selection of risk assessment methodology | |
| **Risk and vulnerability analysis** | Identification of hazards and threats (and opportunities) | -Selection of methodology<br>-Covers both safety and security<br>-Stimulate good discussion<br>-Expose “unknown” hazards | Argumentation for selected method | |
| | Consequence evaluation | -Selection of methodology<br>-Barriers, assessments of barriers (functions, systems, influencing factors)<br>-Vulnerability analysis<br>-Consequence characterisation assessment (damage categories, and also aspects such as ubiquity, persistency, and mobilization) | - Argumentation for selected methods<br>Tools for facilitation of the assessment process | |

# Sikkerhet / Security

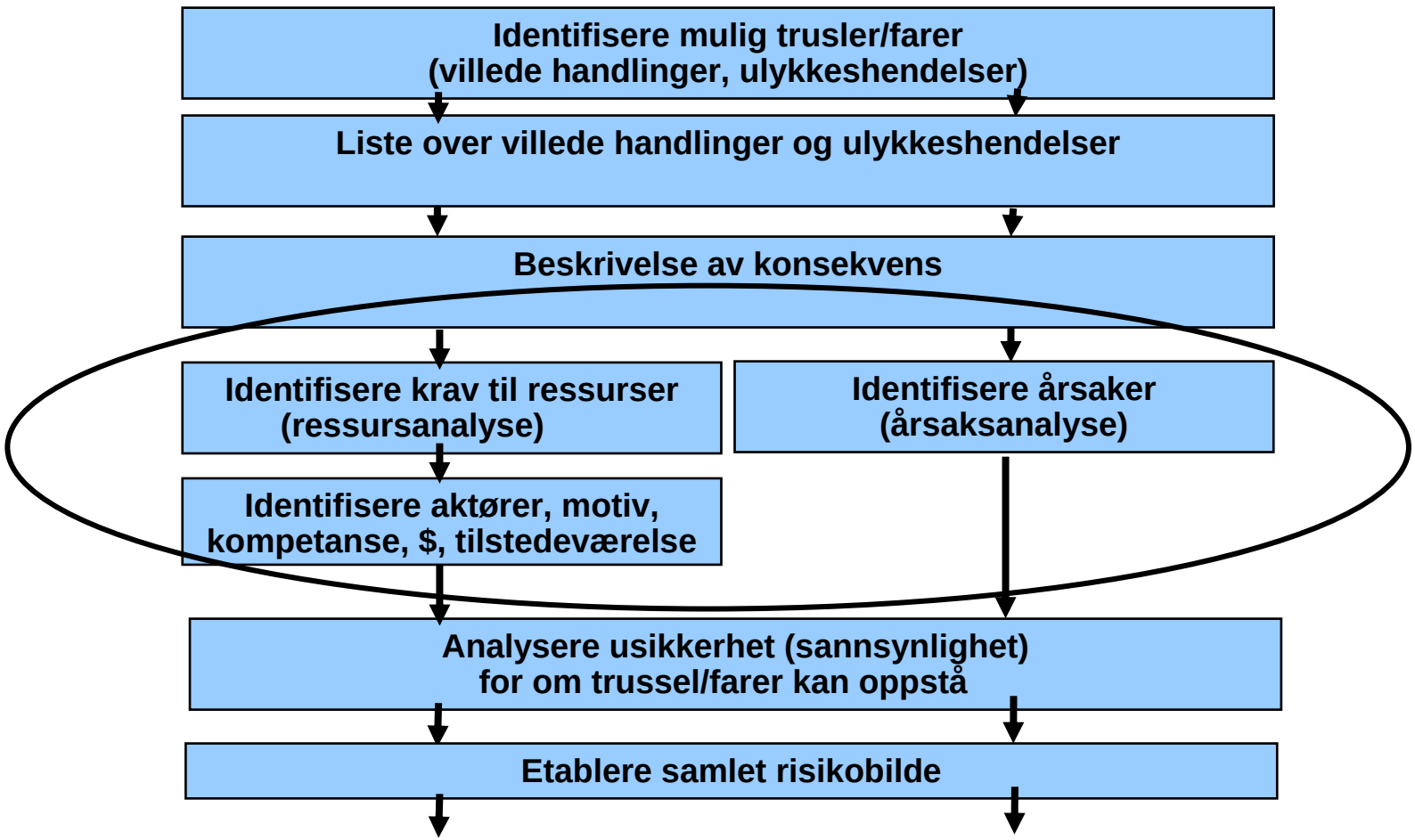
SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

- Risiko og sårbarhetsanalyse som omfatter både villede handlinger og ulykker

proactima
PRO-ACTIVE MANAGEMENT

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

## Risiko og Sårbarhetsanalyse




proactima
PRO-ACTIVE MANAGEMENT

# Erfaringer

# Utfordringer knyttet til IKT

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

- Komplekse systemer
- Vanskelig å få oversikt
- Mangler systemtegninger
- Mangler data
- Villede handlinger

proactima
PRO-ACTIVE MANAGEMENT

# Utfordringer knyttet til ROS analyser

SEROS
SENTER FOR RISIKOSTYRING OG SAMFUNNSSIKKERHET

- Hva er vanskelig
  - Risiko; hva er det
  - Klassifisering
  - Etablering av risikomatrisen
  - Beslutningskriterier/akseptkriterier
  - Plassering av hendelser i en risikomatrise

- Lett å gjøre “feil”

proactima
PRO-ACTIVE MANAGEMENT

# Muligheter

SEROS
SENTER FOR RISIKOSTYRING
OG SAMFUNNSSIKKERHET

- Det er gjort mye bra arbeid
- Det eksisterer mange verktøy
- Det er mye å lære fra andre bransjer/fagområder

men

Det er stor utfordring i etablere et system som er praktisk anvendbart og som kan bidra til at virksomheter med begrenset erfaring kan gjennomføre ROS analyser på en god måte

proactima
PRO-ACTIVE MANAGEMENT

# SEROS

***"En ny tilnærming til risikostyring og samfunnssikkerhet".***

**Ta kontakt med oss på:**
**www.seros.no**