Continuation of the Swedish Civil Contingencies Agency (MSB) methodological support for Information Security Management Systems (ISMS) MSB:s metodstöd

Carina Bengtsson, Daniel Bosk and Lennart Franked[2]

Department of Informationsystems and Technologies
Mid Sweden University, Sundsvall.

April 24, 2017

1. Analysis
   - Organisational Analyses
   - Risk analysis
2. Gap Analysis
   - What is a gap analysis?
   - How should it be done?
   - The checklist
   - Practical Implementation
   - Overview of ISO 27002
   - Results
3. Establish
   - Measurement
   - Processes
   - Governance documents
4. Implementation
   - Plan the implementation
   - Construct and procure
   - Implement
5. Follow Up
   - Monitor
   - Review
   - Top Management Review
6. Improve
   - Improve ISMS and the protection
   - Communicate the improvements

Översikt

What needs protecting?

- What informational assets do we have, and how much are they worth protecting?
- Should lead to a structured list over
  - what informational assets there are,,
  - what requirements and expectations they have, and
  - the worth of each asset.

Finding the informational assets

- Previous process mappings?
- Department wise?
- IT-system?
- Project?
- Processes?
- By function?

MSB:s suggestion on a classification model

Säkerhetsaspekt / Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar*	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. **	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. **

Figure: MSB:s suggestion on a classification model.

University's adaptation of a classification model.

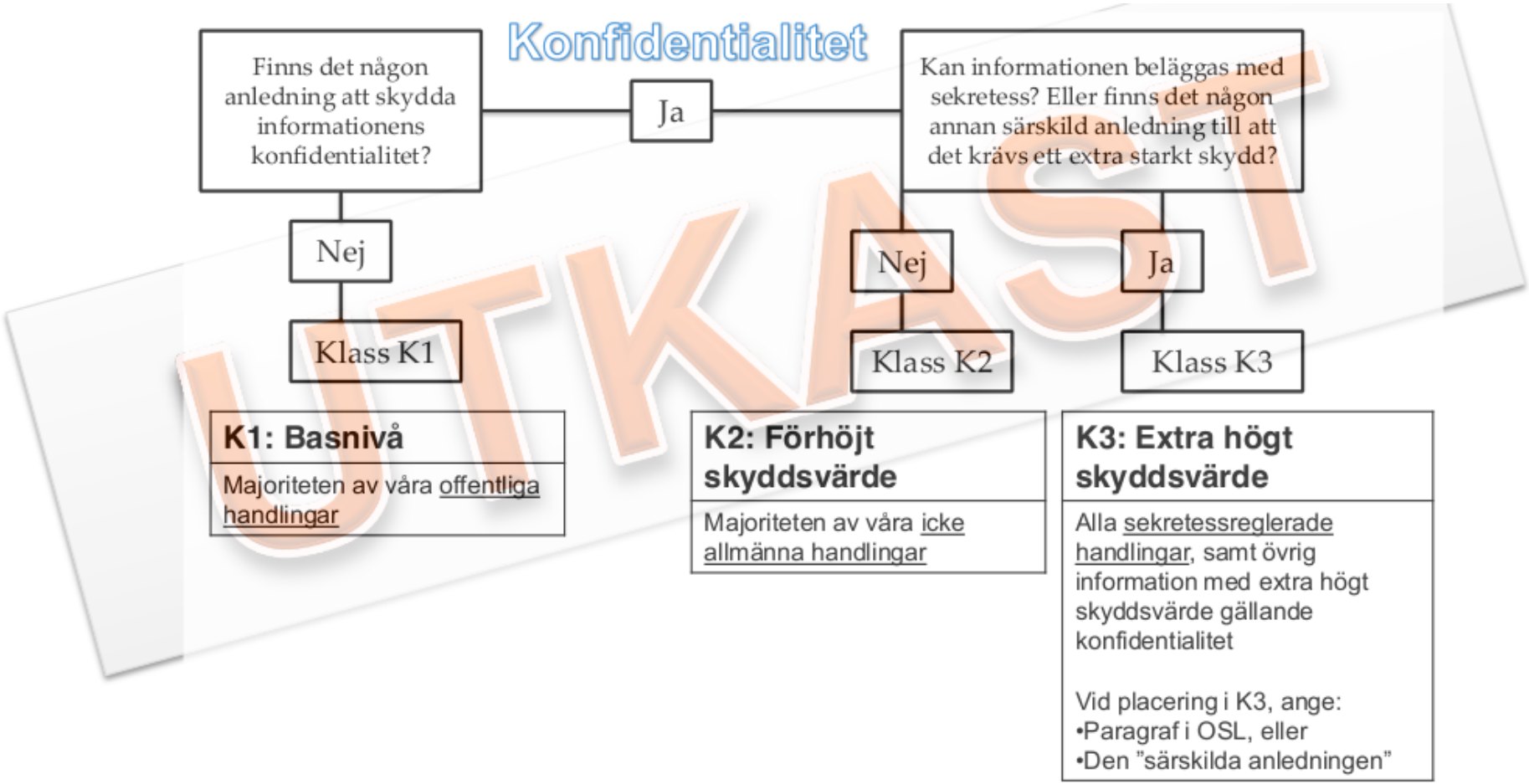


Figure: University's adaptation of a classification model from the confidentiality perspective.

- Used to adapt the protection based on the assets of the organisation.
- Generate a list over
  - existing threats,
  - consequences of the threats, and
  - suggestions for risk management.

Risk matrix

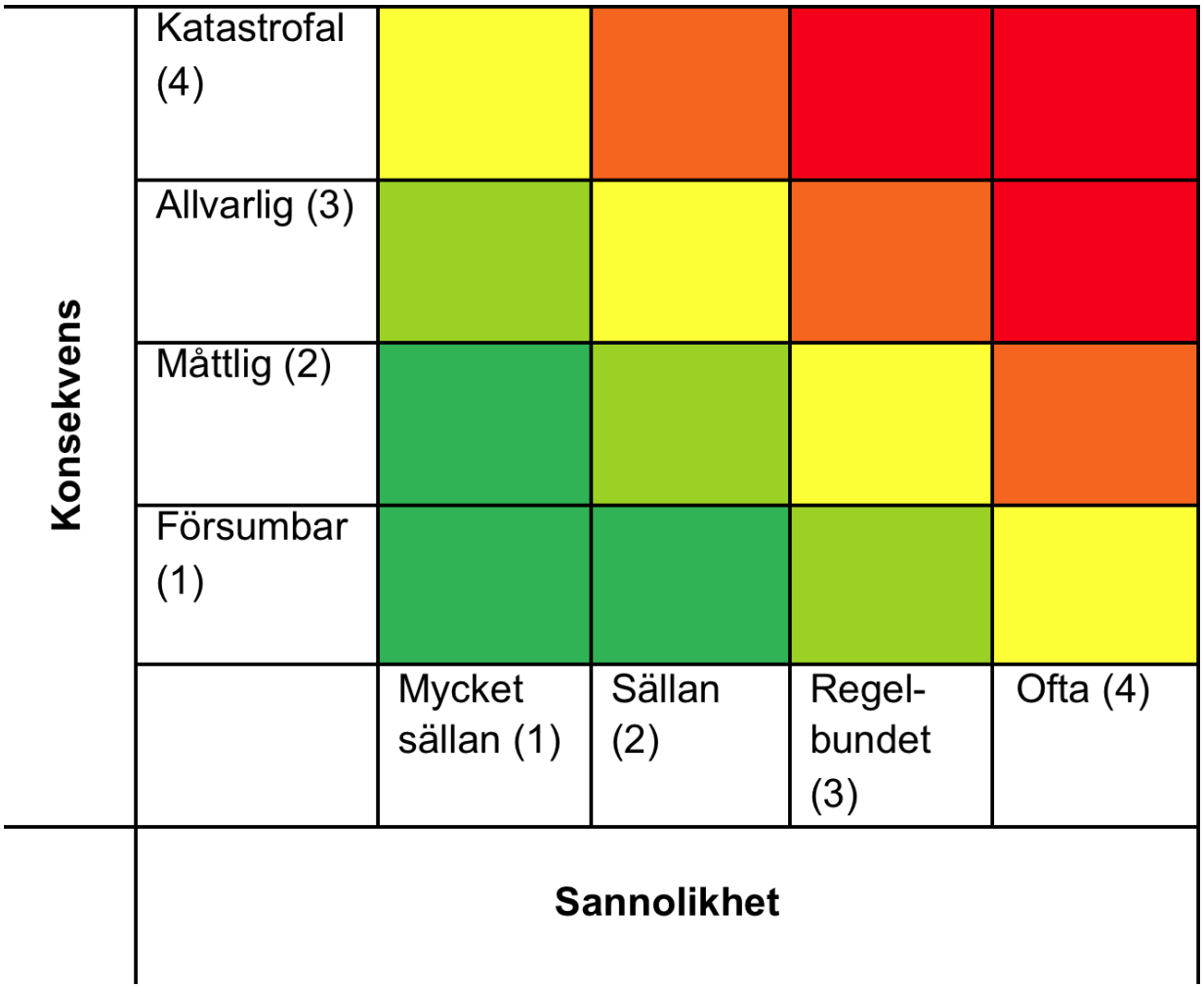


Figure: A risk matrix.

Formal methods?

- There are a lot of research done regarding how to perform risk analysis.
- They can, however be difficult to use.

Översikt

- Analyses the gap between the organisations current information security, and its set goals.
- The methodological support from MSB uses the norm described in ISO 27002, instead of the goal of the organisation.
- The following result will therefore show how the organisation stands in comparison to the expectations in ISO 27002.

Investigates what security measures that

- exists and working,
- exists but doesn't work,
- doesn't exist,
- isn't needed.

When is a gap analysis performed?

- If you want to establish an ISMS.
- If you want to measure, audit or verify the information security level of the organisation.
- If you want to establish requirements on your information security level.

Requirements for performing a gap analysis

The project leader of the analysis task must

- know the organisations need and requirements,
- know any existing governance documents regarding the security work in the organisation,
- have a good knowledge and understanding of the norms in the standard.

- There must exist a clear decision that a gap analysis should be performed,
- Otherwise there must exist a clear mandate to be able to make this call.
- As a support, use MSB:s checklist for gap analysis [And+11].

- Based on ISO 27002.
- Contains 133 security measures.
- Each security measure have one or several questions that helps set the level, based on a scale between 0-3.
- Each security measure belongs to a section.
- Each section belongs to a chapter (area/field).
- There are in total 11 chapters.

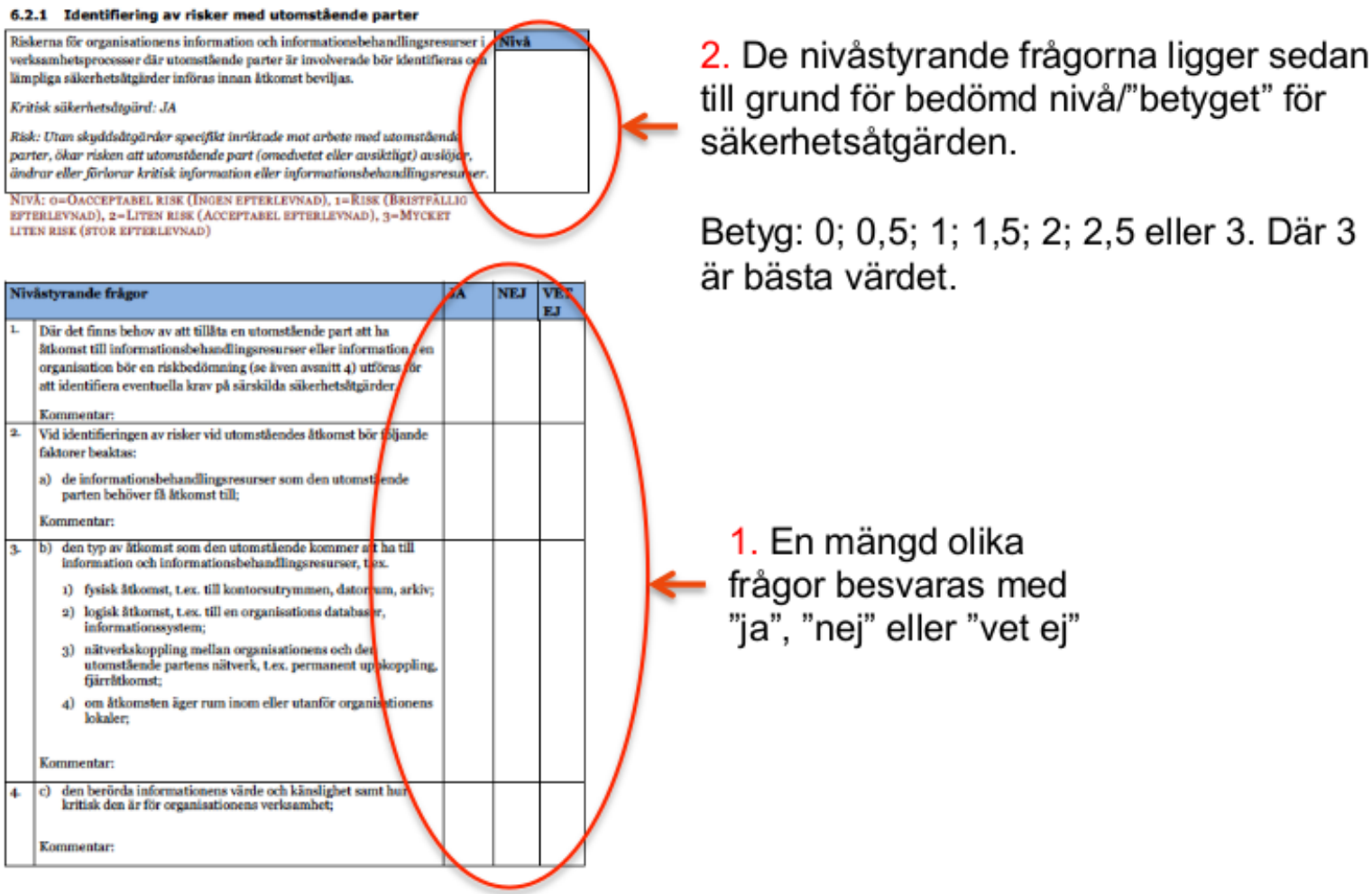
- Out of a total of a 133 security measures, 62 (55) are deemed critical.
- The critical measures is used as a lowest acceptable level for the information security.

Who?

- Analysis leader.
- Experts in the organisation that is most suitable to answer each field in the checklist.
- Doesn't necessarily need to be the managers.

- Book a meeting with the experts.
- Send the questions to the experts in advance.
- At the meeting: Work through all the questions.

Level setting questions



6.2.1 Identifiering av risker med utomstående parter

Riskerna för organisationens information och informationsbehandlingsresurser i verksamhetsprocesser där utomstående parter är involverade bör identifieras och lämpliga säkerhetsåtgärder införas innan åtkomst beviljas. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan skyddsåtgärder specifikt inriktade mot arbete med utomstående parter, ökar risken att utomstående part (omedvetet eller avsiktligt) avslöjar, ändrar eller förlorar kritisk information eller informationsbehandlingsresurser.*	Nivå

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Där det finns behov av att tillåta en utomstående part att ha åtkomst till informationsbehandlingsresurser eller information i en organisation bör en riskbedömning (se även avsnitt 4) utföras för att identifiera eventuella krav på särskilda säkerhetsåtgärder. Kommentar:			
2.	Vid identifieringen av risker vid utomståendes åtkomst bör följande faktorer beaktas: a) de informationsbehandlingsresurser som den utomstående parten behöver få åtkomst till; Kommentar:			
3.	b) den typ av åtkomst som den utomstående kommer att ha till information och informationsbehandlingsresurser, t.ex. 1) fysisk åtkomst, t.ex. till kontorsutrymmen, datorrum, arkiv; 2) logisk åtkomst, t.ex. till en organisations databaser, informationssystem; 3) nätverkskoppling mellan organisationens och den utomstående partens nätverk, t.ex. permanent uppkoppling, fjärråtkomst; 4) om åtkomsten äger rum inom eller utanför organisationens lokaler; Kommentar:			
4.	c) den berörda informationens värde och känslighet samt hur kritisk den är för organisationens verksamhet; Kommentar:			

2. De nivåstyrande frågorna ligger sedan till grund för bedömd nivå/"betyget" för säkerhetsåtgärden.

Betyg: 0; 0,5; 1; 1,5; 2; 2,5 eller 3. Där 3 är bästa värdet.

1. En mängd olika frågor besvaras med "ja", "nej" eller "vet ej"

Figure: Level setting questions that gives an estimate value of security measures.

OBS! Påhittade siffror		2012		
Kaptiel nr:	**Kapitel**	**Kapitel**	**Avsnitt**	**Del-avsnitt**
5	**Säkerhetspolicy**	1,0		
5.1	**Informationssäkerhestpolicy**		1,0	
5.1.1	Policydokument för informationssäkerhet			1,0
6	**Organisation av informationssäkerheten**	1,5		
6.1	**Intern organisation**		1,0	
6.1.1	Ledningens engagemang för informationssäkerhet			1,5
6.1.3	Tilldelning av ansvar för informationssäkerhet			1,5
6.1.4	Godkännandeprocess för informationsbehandlingsresurser			0,5
6.1.9	Oberoende granskning av informationssäkerhet			0,5
6.2	**Utomstående parter**		2,0	
6.2.1	Identifiering av risker med utomstående parter			2,0
6.2.3	Hantering av säkerhet i tredje partsavtal			2,0

Figure: The grade of the section is based upon the grades of each subsection

OBS! Påhittade siffror		2012		
Kaptiel nr:	**Kapitel**	**Kapitel**	**Avsnitt**	**Del-avsnitt**
5	**Säkerhetspolicy**	1,0		
5.1	**Informationssäkerhestpolicy**		1,0	
5.1.1	Policydokument för informationssäkerhet			1,0
6	**Organisation av informationssäkerheten**	1,5		
6.1	**Intern organisation**		1,0	
6.1.1	Ledningens engagemang för informationssäkerhet			1,5
6.1.3	Tilldelning av ansvar för informationssäkerhet			1,5
6.1.4	Godkännandeprocess för informationsbehandlingsresurser			0,5
6.1.9	Oberoende granskning av informationssäkerhet			0,5
6.2	**Utomstående parter**		2,0	
6.2.1	Identifiering av risker med utomstående parter			2,0
6.2.3	Hantering av säkerhet i tredje partsavtal			2,0

Figure: The grade of the chapter is based upon the grades of each section.

Summarizing the grades.

OBS! Påhittade siffror		2012		
Kaptiel nr:	Kapitel	Kapitel	Avsnitt	Del-avsnitt
5	Säkerhetspolicy	1,0		
6	Organisation av informationssäkerheten	1,0		
7	Hantering av tillgångar	2,0		
8	Personalresurser och säkerhet	1,4		
9	Fysisk och miljörelaterad säkerhet	2,5		
10	Styrning av kommunikation och drift	0,3		
11	Styrning av åtkomst	0,0		
12	Anskaffning, utveckling och underhåll av informationssystem	1,5		
13	Hantering av informationssäkerhetsincidenter	1,3		
14	Kontinuitetsplanering för verksamheten	1,0		
15	Efterlevnad	1,3		

1,2

Figure: The total grade is based upon the grades of each chapter.

1. Security Policy
2. Organisation surrounding information security.
3. Management of assets.
4. Human resources and security
5. Physical and environmental security
6. Control of communication and management.
7. Access control.
8. Acquiring, developing and maintaining information systems.
9. Managing information security incidents.
10. Contingency planning for the organisation.
11. Compliance.

- What is the directional intent for the organisation in regards to information security.
- How should this be achieved.
- Short explanation of terminology
- How will the responsibility be divided.
- Legal and internal requirements should be taken into account.

- Should exist a framework within the organisation that is controlling the information security.
- Decisions need to be taken regarding governance documents.
- Clearly stated how responsibilities are divided.
- Contains six critical security measures.

- Ensuring that the assets in the organisation should have a suitable protection.
- Contains two critical security measures: List of assets and guidelines for classifying assets.

- What to take into account before, during and after employment within the organisation.
- Background checks, in house training, how to handle permissions when an employment has been ended.
- Contains three critical security measures.

- To prevent unauthorized access.
- Reduce the risk of damage on informational assets.
- Contains four critical security measures.

- Resources that are managing information should have a safe and reliable operation.
- Clearly state the responsibilities and the documentation for this.
- Have 14 critical security measures.

- Access to the system should be controlled through the organisational and security requirements.
- Contains ten critical security measures.

- Ensure that new and existing information systems are keeping a high security level.
- Contains seven critical security measures.

- Security incidents should be handled.
- Reduce the risk of an incident happening again.
- Contains two critical security measures.

- Prevent disruptions in the organisation.
- Learn how to deal with disruptions.
- Contains three critical security measures.

- Ensures that the organisation comply to the external and internal requirements that exist in regards to information security.
- Contains three critical security measures.

Result of the gap analysis

- Which security measurements are implemented?
- What are the scope and quality on the implemented measurements?
- What weaknesses and strength are there on the implemented measurements?
- What is the next step?

- How well have the work been done?
- What are the input values that have been used?
- What is the result of the analysis?
- Summary of the entire work.
- Suggestions on how to continue.

Översikt

How to choose the security measurement

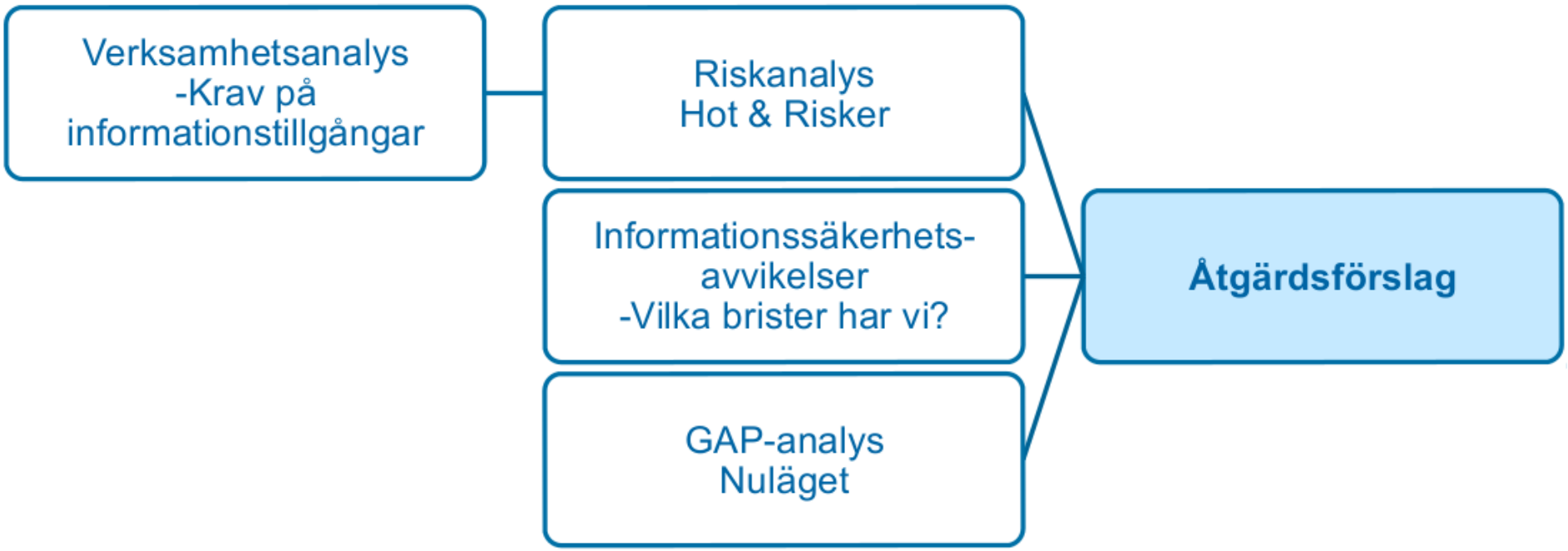


Figure: Choosing security measures.

Best practice Based upon different security measures listed in ISO 27002.

Risk analysis Tailored security measures based solely on organisations need.

- Base analysis – the need for protection.
- Will the protection have wished effect?
- Focus on *if* they should be implemented, not *how*.

Type of measurements

- Governance documents.
- Analysis, monitoring.
- Technical protection.
- Education.
- Processes.

Develop security processes

- Collection of activities that manages a defined need.
- Integrate with existing processes.
- For example ISMS.
- Examples: Information security classification, access control.

- Wide competence.
- Representatives from the entire (affected parts) organisation.
- Makes it easier to coordinate with existing processes.

Develop governance documents

- Start with one policy, what is the directional intent of the organisation.
- Identify existing documents: revise, revoke, introduce new.
- Adapt based on the current document structure.

Don't forget

- version control,
- document owner,
- decision date,
- who took the decision.

They should be written in such a way that everyone can understand them

Översikt

- At this stage security processes are formed and decisions have been made for taking security measures.
- Can be done in project form, or just incorporated into the regular work load.

Plan the implementation

- Should something be prioritized?
- Do some implementation measures dependend on others?
- What can be constructed, and what can be procured?
- Need a time plan, and ensure everyone is aware that the work will start.

Construct The organisation to in-house development.

Procure The organisation procures solutions.

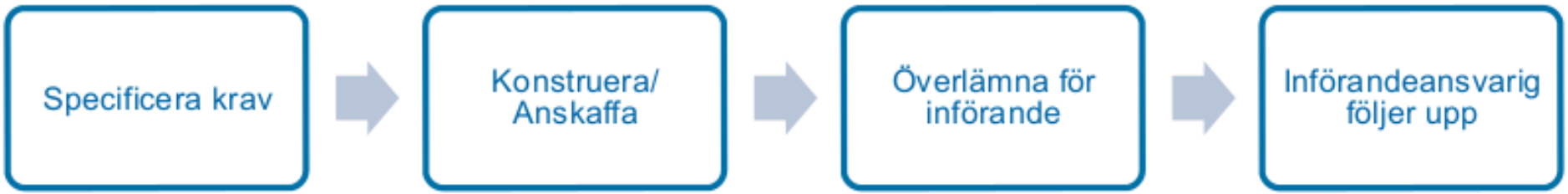


Figure: Process to construct and procure.

- Important clearly have stated what requirements exist.
- IT-department are unaware of how much the information they are managing is worth protecting – Need to be specified.
- Think about usability to ensure that the organisation do not circumvent the measures.

Implement

- One coordinator.
- Multiple persons responsible for the practical.
- The work is carried out in groups: Include area managers that are affected by the security measures.

Groups responsible for implementing the security measures

Focus on:

- Representation of the entire organisation.
- Do the employees need training? They need to be able to use and understand the security measures.
- Who should manage the security measures? There is a need for a management plan.
- Ensuring that the organisation will embrace the measures.

Changing the behaviour

- Many security measures needs a change in the behaviour to work.
- Communicate and explain *why* – Make sure the explanation is targeted.

Översikt

Monitor

- Should be done continuously in different levels in the organisation.
- Will be used as a base for further analysis of the security measure, and for presenting to the top management.

Ensure that the right conditions exist for evaluation:

- Effect of ISMS: Are there sufficient measurements in place towards the current threats?
- Effect of the security measurements: Have they been implemented?
- How have the informational assets been affected: Have the secrecy become greater?

- A part of the monitoring, which purpose is to discover new threats.
- Discover any shortcomings in the measurements taken for previously known threats.
- This also includes fixing these shortcomings.

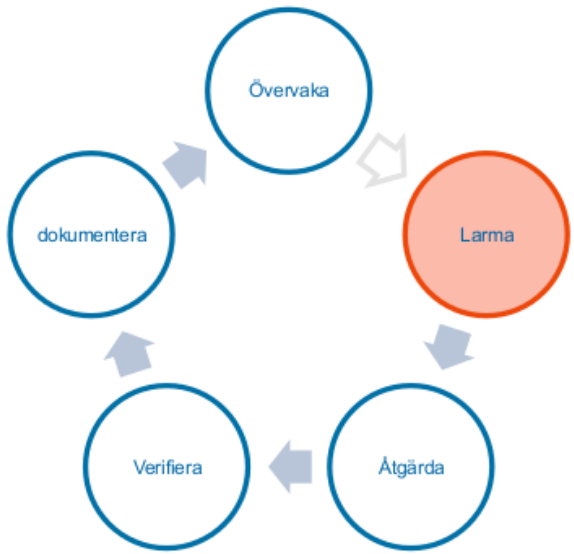


Figure: Cycle for monitoring and incident management.

- A deeper analysis of the result from the monitoring.
- Part of the recurring organisational follow-ups, for example internal revision.
- Use the information from the monitoring as base.
- Is the ISMS working?

- ISO 27001: the top management must ensure this is done – and should take part of the result.
- How?
  - Use ISO 27001 ISMS.
  - Use ISO 27002 for the security measures.
- Who? Independent auditor with the support from those who are responsible for the ISMS.

Top Management Review

- The top management are responsible for the entire organisation.
- It is important that they understand the result of the audit.
- Recommended to have a yearly review of the information security.

- Should be given by the person responsible for the information security, along with the experts from the GAP-analysis.
- Should be done yearly.

- Should include the result of the audits, weaknesses and threats that haven't been fully covered from the last risk assessment.
- Should result in decisions regarding how to improve the result of the ISMS, update of risk assessment and risk treatment plan.

Översikt

Improve ISMS and the protection

- Use the result from follow-ups and the top management review.
- Recommended that the process is done in a structured way, PDCA
- Standardise: Establish the measures in the governance documents, ensure that they are implemented correctly.

Communicate the improvements

Try to create an interest that ensures that the

- employees *will learn*,
- get a *positive* attitude towards information security,
- have an *intention* to work towards improving the information security,
- and changes their behavior.

[And+11] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson, and Kristina Starkerud. *Gapanalys – Checklistan*. Dec. 2011. URL: http://www.informationssakerhet.se.