CoolWave AB

Cyber Security
Informationssäkerhet

ISO27001, ISA/IEC 62443, NIST, Common criteria, NIS-Direktivet, Säkerhetskyddslagen, GDPR-Direktivet.

Varför InfoSäk?

Trender:

- Uppkoppling av i stort sett allting
- Integration av i stort sett allt
  (även system som tidigare var isolerade)
- Exponeringsytan för angrepp ökar
- Cyberhoten blir allt mer komplexa och potenta
  - Spioneri
  - Terrorbrott
  - Ekonomisk brottslighet
  - Prisjägare
- Utförs av:
  - Enskilda hackers
  - Organiserad brottslighet
  - Statligt organiserad terror
  - Statligt organiserad krigföring mot civilsamhället
    (inte bara av illasinnande stater)

Vad vi kan göra:

- För att skydda kritiska tillgångar, måste vi skilja på information och system.
- Vi måste också bättre förstå vad vi har för information, hur vi bäst skyddar den och var vi kan lagra och hantera den.
- Teknisk IT-Säkerhet är viktigt, men bara en del av en helhet.
- Informationssäkerhet eller ”eGovernance” ger management direktkontakt med verkligheten!

Olika perspektiv

- Cybersäkerhet
- IT-Säkerhet
- Informationssäkerhet
- Datasäkerhet
- Betalningssäkerhet PCIDSS
- Säkra Industriella System (ICS)
- Kritisk Infrastruktur (NIS-Direktivet)
- Personuppgiftssäkerhet (GDPR-Direktivet)

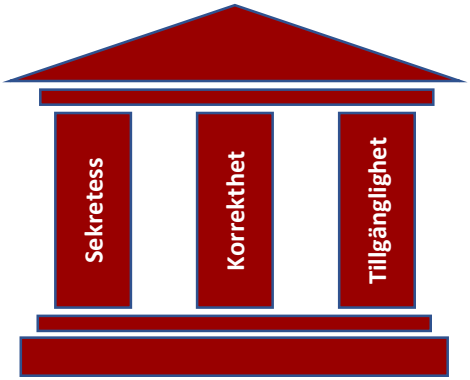
Dilemmat

- I generaliserande termer är vi ganska bra på IT-Säkerhet i Sverige, tror vi.
- Därför underskattar vi betydelsen av Informations-säkerheten som helhet!
- På följande sidor beskrivs helheten av Informationssäkerhet.

CIA-Triaden

De tre grundpelarna inom Informationssäkerheten:

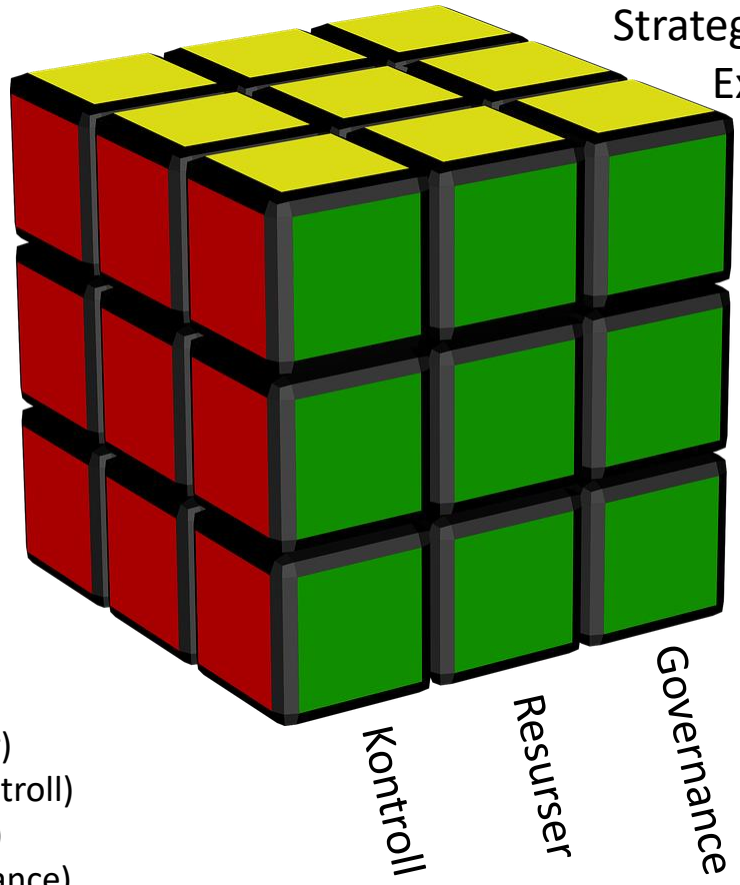
- Confidentiality – Sekretess
- Integrity – Korrekthet
- Availability – Tillgänglighet



Mekanismer:

- Symetrisk kryptering ger sekretess
- Asymetrisk kryptering ger manipulationsskydd och säkerhetsstyrning
- Autentisering – Säkerställer identiteter
- Backup av data och informationer säkerställer tillgänglighet
- Redundans av system och kommunikationsvägar skapar tillgänglighet

Inte bara teknik

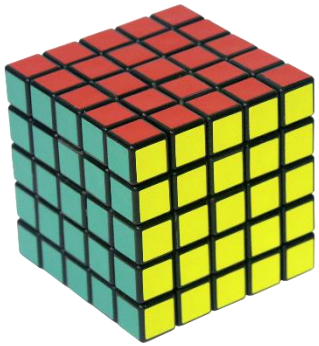


Man kan tillfoga:

- Kompetens (ingår i resurser)
- Mäta prestanda (ingår i kontroll)
- Prioritering (ingår i strategi)
- Förbättring (ingår i governance)

Perspektiv och aspekter

- Symetrisk kryptering
- Asymetrisk kryptering
- Autentisering
- Backup
- Redundans



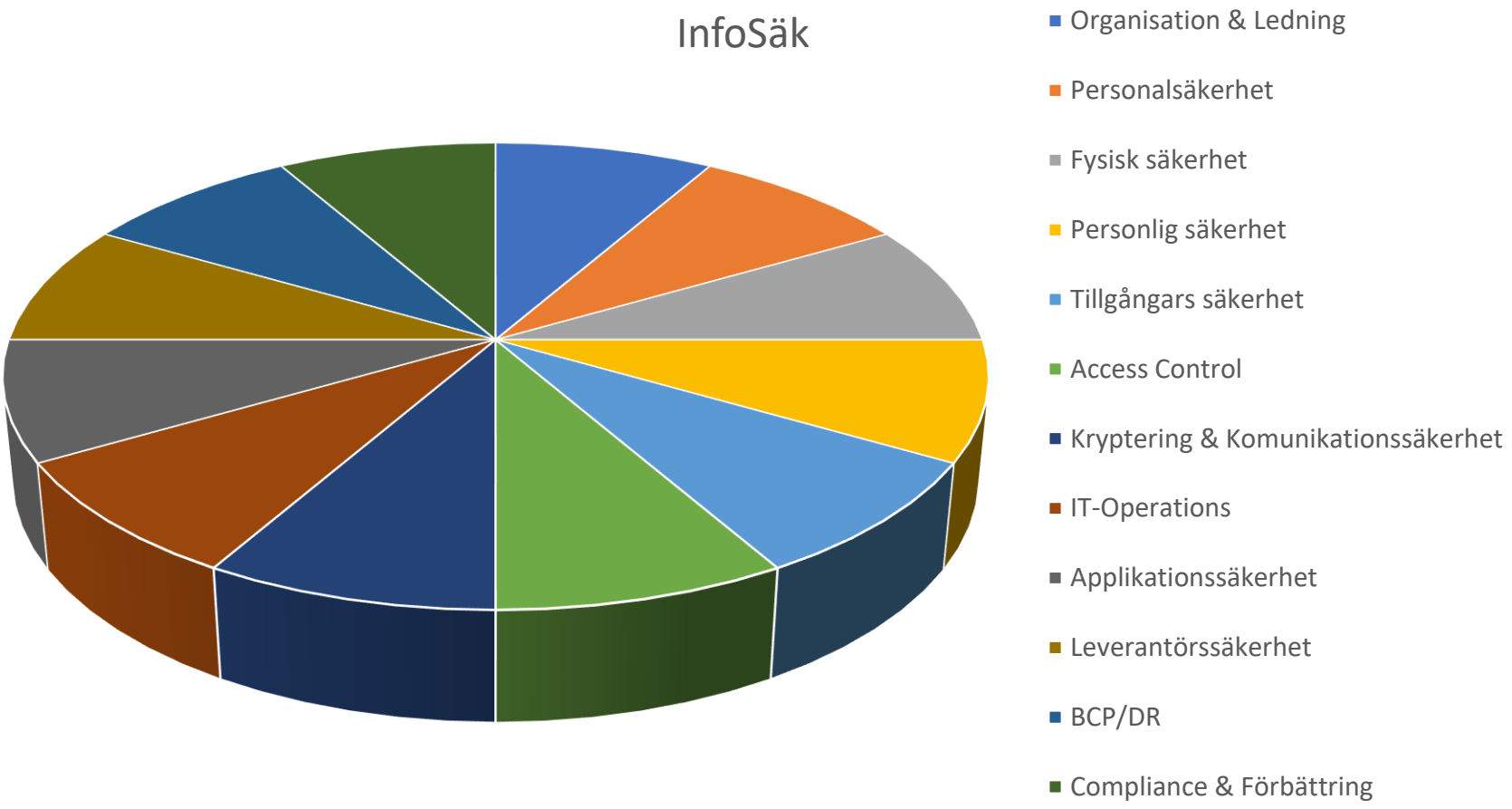
- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability

- Algorithmer & metoder
- Nycklar & Certifikat
- Säkerhetsmanagement
- Utbildning & träning
- Kontinuerlig förbättring
- Kontroller

ISO/IEC 27001 Standarden

- Organisationens förutsättningar
- Ledarskap
- Planering – (Riskhantering+Mätbara mål)
- Stöd – (Resurser/Kompetens/Medvetenhet/ Kommunikation/Dokumentation)
- Verksamhet (Säkerställande av Processer)
- Utvärdering av prestanda
- Förbättringar (Avvikelsehantering)

Appendix A / ISO27002



LIS - Dokumentationsstruktur

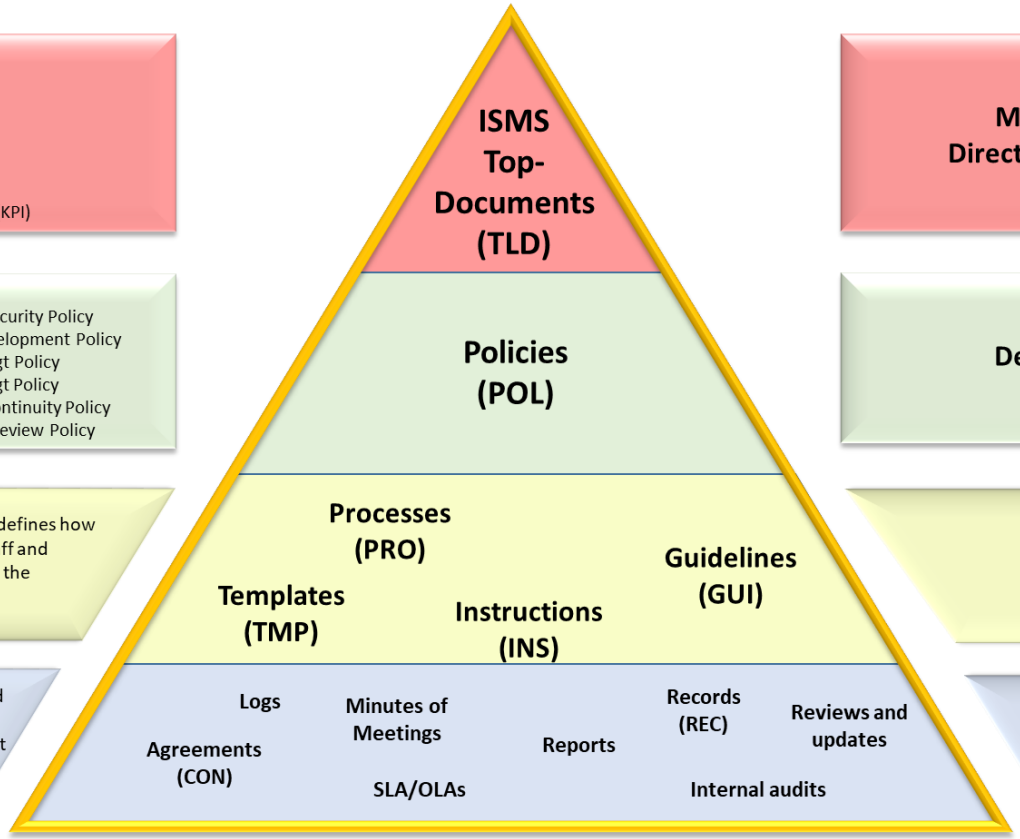
Top Level Documents:
1) Scope of ISMS
2) Information Security Policy (ISP)
3) ISMS Organisation
4) ISMS Documentation Framework
5) Risk Management Framework
6) Statement of Applicability (SoA)
7) ISMS Objectives and Key Performance Indicators (KPI)

Examples of Policies:

A7. HR Security Policy	A13. Network Security Policy
A8. Asset Management Policy	A14. Secure Development Policy
A9. Access Control Policy	A15. Supplier Mgt Policy
A10. Cryptography Policy	A16. Incident Mgt Policy
A11. Physical Security Policy	A17. Business Continuity Policy
A12. IT-Operations Policy	A18. Audit and Review Policy

Processes, Guidelines, Instructions & templates, defines how information security is implemented and how staff and management should act in order to keep up with the information security policy and procedures.

Records, logs, agreements, meeting protocols and other evidence proves that the ISMS is kept alive. Periodic Internal audits and reviews are important to maintain and improve the seucurity and awareness throughout the organisation.



Managements Directive & Resources

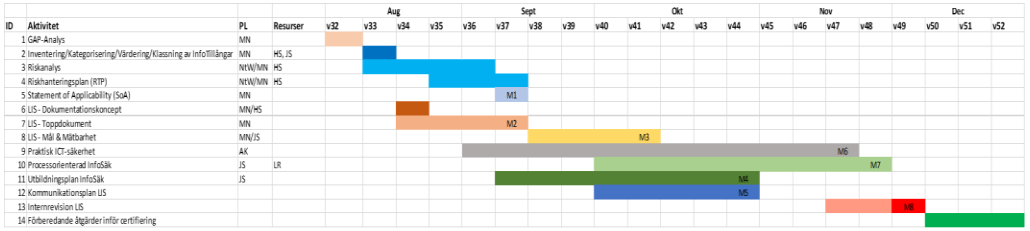
Defines ”What”

Defines ”How”

Documented evidence proves compliance

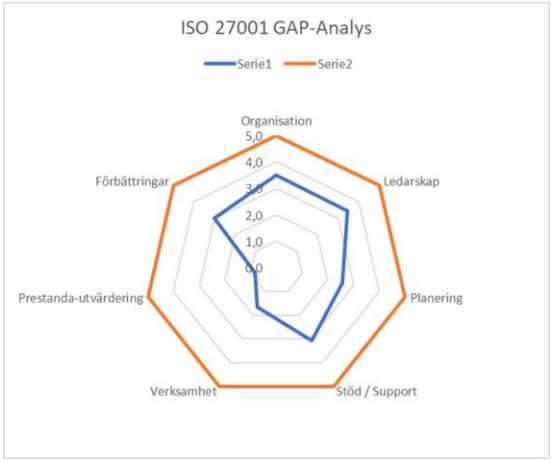
Exempel på projektplan

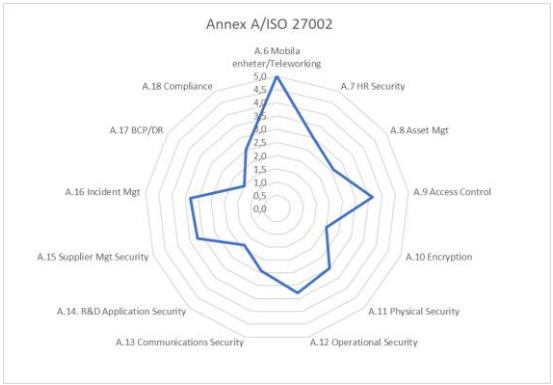
- GAP-Analys ISO27001
- Upprättande av projektplan
- Inventering av tillgångar
- Inrättande av Klassificeringsmetodik
- Klassning & värdering av tillgångar
- Riskanalys
- Riskhanteringsplan
- Statement of Applicability
- Kommunikationsplan
- Utbildningsplan
- Implementering/verifiering av Säkerhetskontroller
- Implementering/Verifiering av InfoSäk-Processer
- Ledningens genomgång
- Internrevision
- Förberedelse inför certifiering



GAP-Analys enligt ISO27001

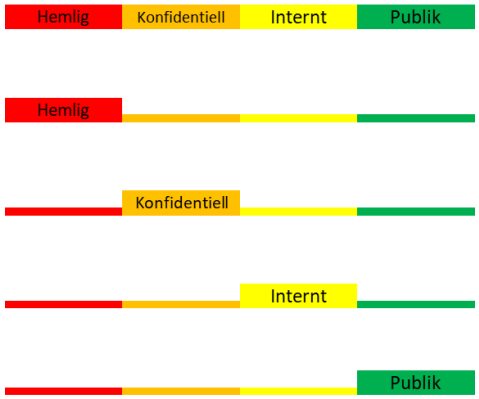
- En GAP-Analys mot ISO27001 brukar ge en bra bild av läget, före och efter åtgärder.





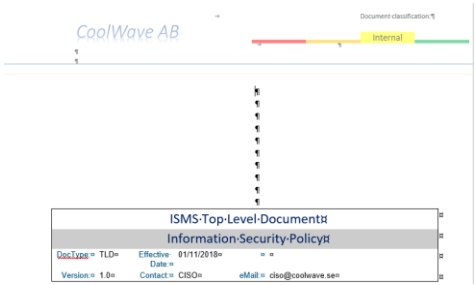
Informationsklassning

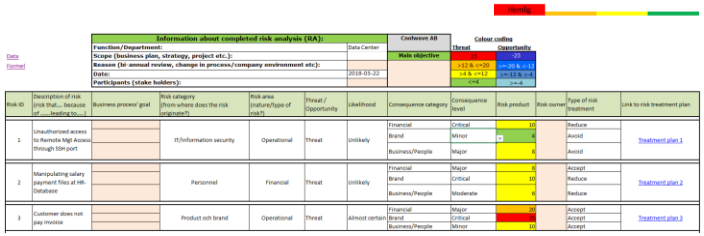
- Informationsklassningsmetod
- Kriterier för resp skyddsklass
- Värderingsregler
- Skyddsregler för hantering
- Skyddsregler för kommunikation
- Skyddsregler för lagring



Märkning

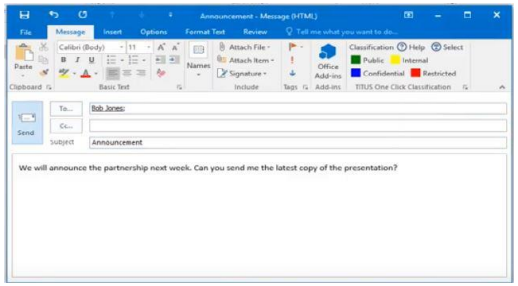
Utskrivna dokument





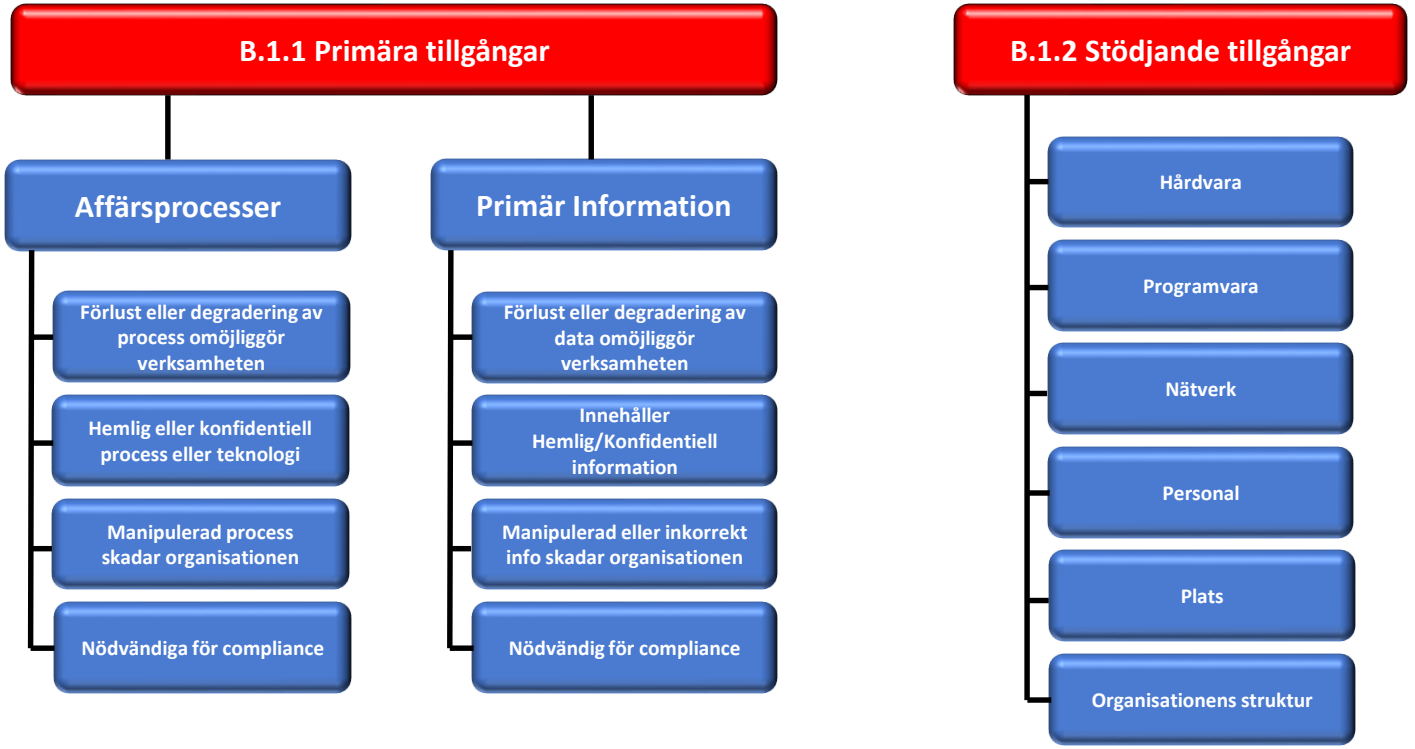
Extern Lagringsmedia

eBrev



USB-Stickor

Identifiering av Informationstillgångar



Ovanstående beskrivning följer ISO/IEC 27005/Appendix B

Informationsinventering

Inventering av tillgångar;

- Informationstyper
- Var/hur lagras info?
- Vem är ansvarig ägare?
- Var/hur hanteras/behandlas info?
- Värdering av info?
- Vilken klass bör väljas för info?
- Informationstillgångar
  - Primära tillgångar
  - Stödjande tillgångar

Vad är risk?

- (Informations-)tillgångar har inre ”Sårbarheter”.
- Hot kommer utifrån i någon form
- Med ”utifrån” menas i tillgångens perspektiv. Dvs yttre hot kan även uppstå inom organisationen eller inom ett system.
- Risk uppstår när;
  Risk = (Inre) Sårbarhet + (yttre) Hot
- Risk kan också kvantitativt beräknas;
  Risk = Hot * Sannolikhet

Olika Riskanalysmetoder

Kvantitativ Riskkalkyl:

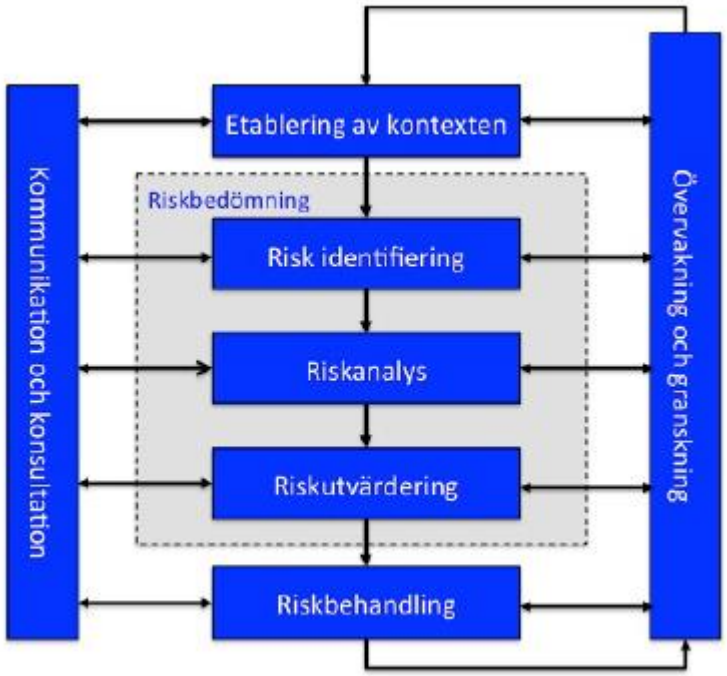
- Tillgångens värde (AV)
- Exponeringsfaktor (EF)
- Kostnad för enskild förlust (SLE=AV*EF)
- Sannolikheten för årlig uppkomst (ARO)
- Sannolik årlig förlust (ALE=SLE*ARO)

Kvalitativ Riskkalkyl:

- Brainstorming/scanarier
- Delphi technique
- Storyboarding
- Focus groups
- Surveys
- Checklists
- Interviews

Riskanalys

- Etablering av kontext
- Riskbedömning
  - Riskidentifiering
  - Riskanalys
  - Riskutvärdering
- Riskbehandling
- Kommunikation
- Övervakning



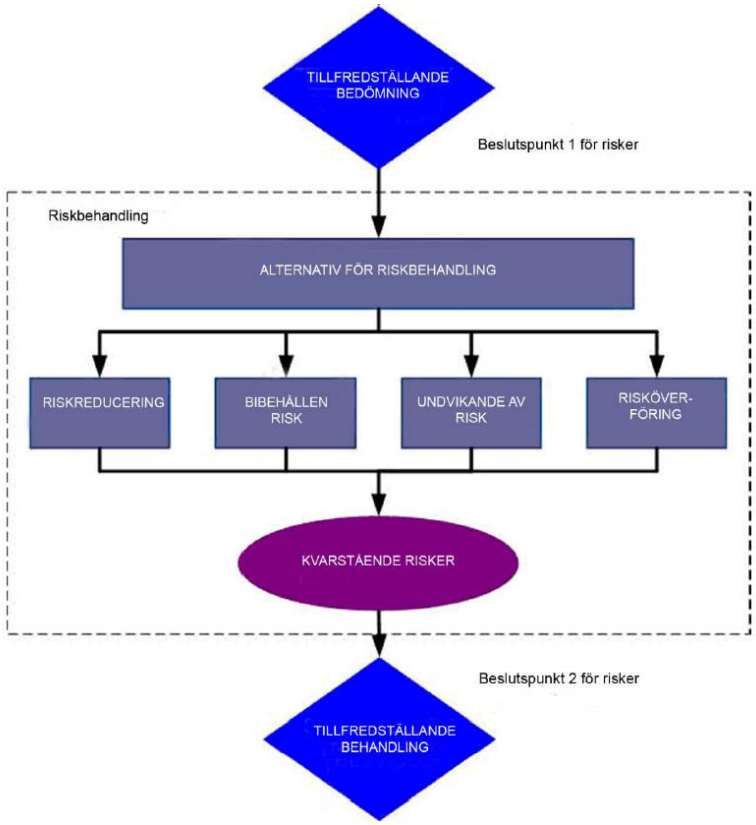
Riskmatris

- När riskregistret är upprättat, skall samliga jämföras så att riskbehandling kan ske i rätt ordning och prioritet.

Risk Matris	Sannolikhet				
Konsekvens	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5

Riskbehandling

- Alternativ
  - Riskreducering
  - Undvikande av risk
  - Risköverföring
  - Bibehållen risk
- Kvarstående risk



Riskhanteringsplan

Data
Formel

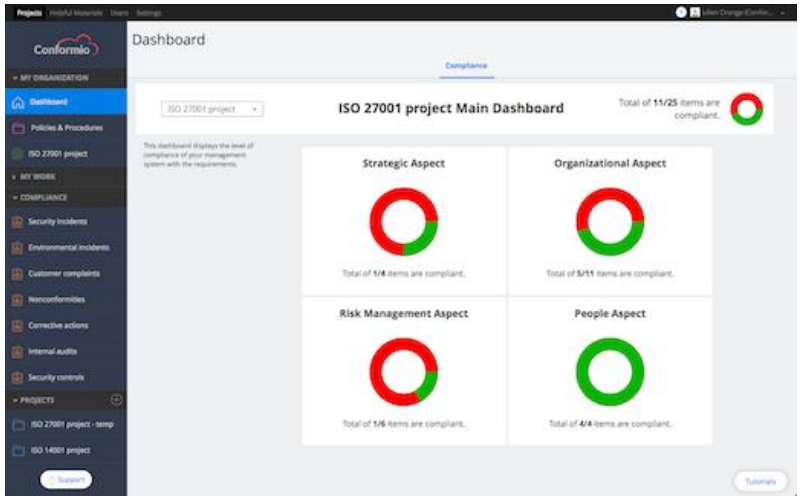
Information about completed risk analysis (RA):		Coolwave AB	Colour coding	
			Threat	Opportunity
Function/Department:	Data Center			
Scope (business plan, strategy, project etc.):		Main objective	25	-25
Reason (bi-annual review, change in process/company environment etc):			>12 & <=20	>=-20 & <-12
Date:	2018-05-22		>4 & <=12	>=-12 & <-4
Participants (stake holders):			<=4	>=-4

Risk ID	Description of risk (risk that…. because of ……..leading to…..)	Business process' goal	Risk category (from where does the risk originate?)	Risk area (nature/type of risk?)	Threat / Opportunity	Likelihood	Consequence category	Consequence level	Risk product	Risk owner	Type of risk treatment	Link to risk treatment plan
1	Unauthorized access to Remote Mgt Access through SSH port		IT/Information security	Operational	Threat	Unlikely	Financial	Critical	10		Reduce	Treatment plan 1
							Brand	Minor	4		Avoid	
							Business/People	Major	8		Avoid	
2	Manipulating salary payment files at HR-Database		Personnel	Financial	Threat	Unlikely	Financial	Major	8		Accept	Treatment plan 2
							Brand	Critical	10		Reduce	
							Business/People	Moderate	6		Reduce	
3	Customer does not pay invoice		Product och brand	Operational	Threat	Almost certain	Financial	Major	20		Accept	Treatment plan 3
							Brand	Critical	25		Accept	
							Business/People	Minor	10		Accept	

- Risklista
- Beskrivning
- Riskprodukt = Sannolikhet * Konsekvens
- Riskägare
- Vald riskhantering

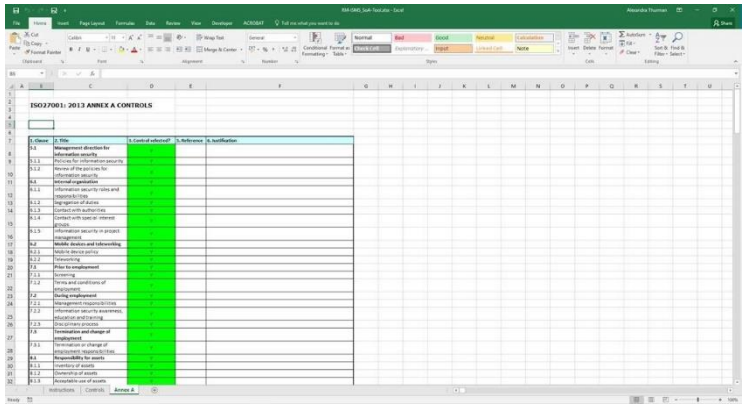
InfoSäk-Mål och KPIer

- Mätbara mål
- Sensorer
- Evidensbaserade resultat
- Presenterade i realtid
  (eller periodisk rapportering)
- Kontinuerlig förbättring



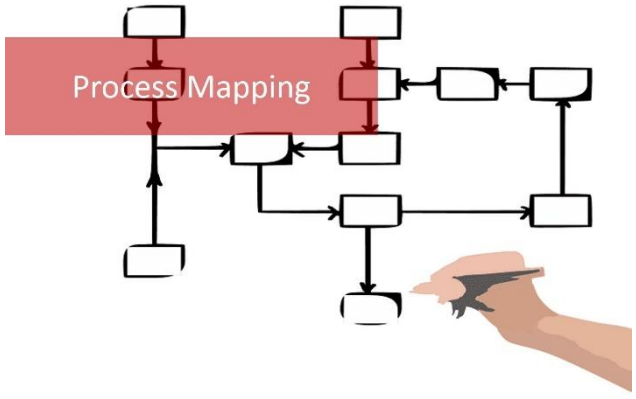
Implementering av Säkerhetskontroller

- Statement of Applicability (SoA)
- Valda säkerhetskontroller
- Tidplan
- Verifiering
- Test
- Dokumentation



InfoSäk-Processer

- Backup och Restore
- Utbildningsplan & Kontroll
- Change Management
- Incidenthantering
- GDPR-Personuppgiftincidenthantering
- Personal on-boarding/terminating
- Leverantörskvalificering/övervakning
- Kontinuitetsplaneprocess
- Internrevision



Vi hjälper er gärna med ert InfoSäk-Projekt

Kontakta oss på:

info@coolwave.se

www.coolwave.se

Tel: 070-595 9492

Frågor?