

NIS2-direktivet och nya Cybersäkerhetslagen

EU-lagstiftning som berör svenska kommuner
och praktiska tips på implementering



Björn Davidsson

Utvecklingschef, Compliance-
ansvarig, Växjö



Agenda

- EU-lagstiftning – fokus säkerhet
- NIS2/Cybersäkerhetslagen
- Implementation – tips/exempel
- ISTs implementation
- Var hittar jag mer information?
- Frågor

Bakgrund

- Digitaliseringen
- Mjukvara
- Hot
- Höja nivån
- Samordning -> Uppföljning



Lagstiftning

GDPR

NIS2

CER



CRA

DORA

AI Act

Lagstiftning



Lagstiftning	Namn (Förordning vs Direktiv)	Innebär	Vem berörs?	Från när?
GDPR	General Data Protection Regulation (F)	Skydd persondata	Personuppgifts-ansvariga- och biträden	2018
CER	Critical Entities Resilience (D)	Öka fysisk motståndskraft hos samhällsviktig verksamhet	Energi, Transport, Vatten, Finans etc	18 Okt 2024
CRA	Cyber Resilience Act (F)	Öka motståndskraft i produkter med digitala inslag	Leverantörer av produkter med digitala element	Antogs 12 mars 2024 – 3 års införande.
DORA	Digital Operational Resilience Act (F)	Öka digital motståndskraft	Finanssektorn och relaterad IKT	16 jan 2023, tillämpning 17 jan 2025
AI Act	AI-förordningen (F)	Harmonisera regler Insyn, kontroll	Producenter, distributörer och användare av AI	1 aug 2024 -> 2 aug 2026 (tillämpning)
NIS2	Nätverk-och informationssystem 2 (D)	Öka Cybersäkerhet Harmonisera införande	Nätverk & informationssystem	17 Okt 2024



NIS2 vs Cybersäkerhetslagen



Väsentlig

Viktig

NIS

Energi

Transport

Bankverksamhet

Finansmarknads-
infrastruktur

Hälsö-och
sjukvård

Vattenförsörjning

Digital
infrastruktur

NIS2

Post-och
budtjänster

Avfallshantering

Kemikalier

Livsmedel

Tillverkning av
medicinsk
utrustning

Förvaltning av
IKT tjänster
(mellan företag)

Offentlig
förvaltning

Rymden

Tillverkning

Digitala
leverantörer

Forskning

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transporter Tillverkning av motorfordon, släpfordon, påhängsvagnar och andra transportmedel
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Vårdgivare i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro diagnostik
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Digitala leverantörer Förvaltning av IKT-tjänster Post- och budtjänster Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Avfallshantering Forskning Lärosäten med examenstillstånd Offentlig förvaltning Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner



Ej retroaktiv

Tillsyn

Vem omfattas?

- Verka inom EU
- Omfattas av någon av de 18 sektorerna
- Minst 50 anställda eller omsättning av 10M €

Undantag

- Verksamheter/Leverantörer av kritiska tjänster omfattas oavsett storlek.



Obligatoriska åtgärder

- Incidenthantering
 - Betydande påverkan
 - 24h – initial varning
 - 1 mån - slutrapport
- Kontinuitetshantering

Övriga åtgärder

- Riskbedömningar
- Tekniska åtgärder
- Organisatoriska åtgärder
- Leveranskedja

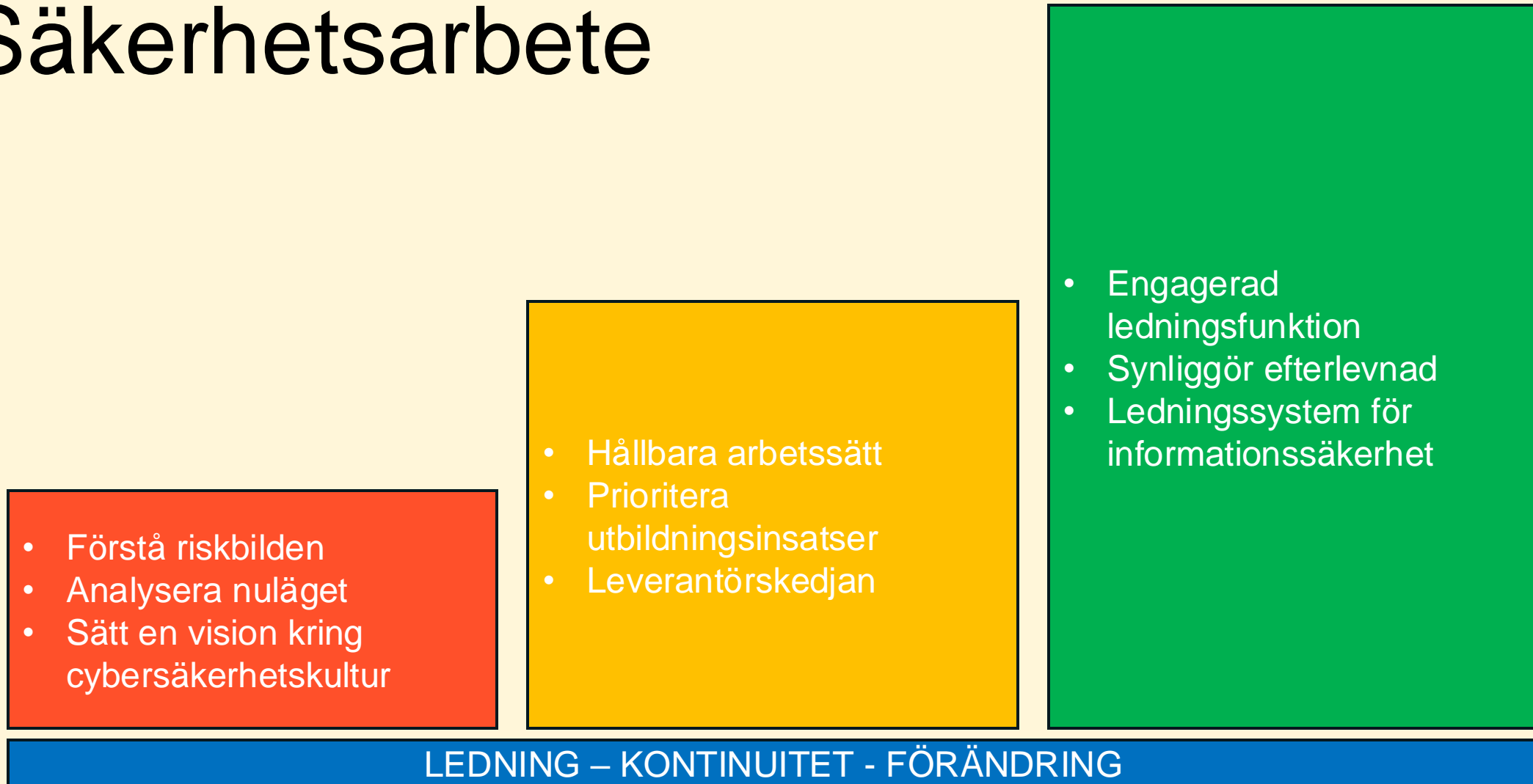




Sanktioner

- Anmärkning
- Förelägganden
- Viten
- Avgifter – Offentlig verksamhet 10MSEK
- Avsättning enskilda ledande personer – gäller INTE offentlig verksamhet

Säkerhetsarbete



Var hittar jag mer information?



Myndigheten för
samhällsskydd
och beredskap



Sveriges
Kommuner
och Regioner

Säkerhetsarbete på IST

- ISO Standarder
- Ledningssystem

ISO 9001
Kvalitet

ISO 14001
Hållbarhet

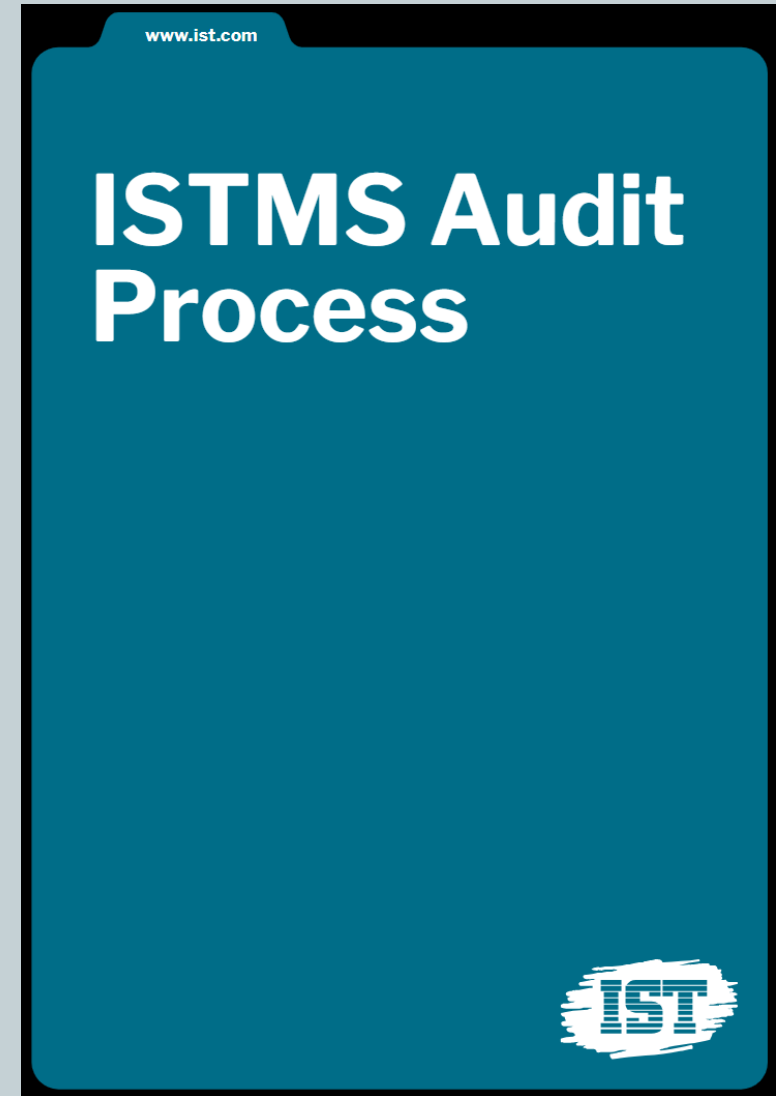
ISO 27001
Informations-
säkerhet

GDPR



Standards & Governance

Styrning & Uppföljning



Compliance work – powered by S&G



Relevant
legislation



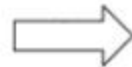
Understand the
legal requirements



Put into IST context



Design procedures
&
guidelines



Awareness
&
training



Accountability
Follow up (Audit)

Dokumenterade rutiner

Guide

Guides typically includes documents that describes or gives an overview of something. These type of documents would typically be suffixed: *Guide*, *Description*, *Map*, *Overview*, *Model* etc.

- [illegible]

Guidelines

Guidelines typically defines rules and regulations that should be followed. These type of documents would typically be suffixed: *Guideline, Statement, Standard or Policy*.

- [Academic Excellence Guidelines](#)
- [Academic Excellence \(B&B\) Informational Website](#)
- [Administrative Guidelines](#)
- [Anti - Sexual Harassment](#)
- [Civility Guidelines](#)
- [Data Management/Access Guidelines](#)
- [Environmental Policy](#)
- [Executive Order](#)
- [General Campus Guidelines](#)
- [Graphic Guidelines](#)
- [Information Security Policy](#)
- [IT Management Plans](#)
- [Library \(B&B\) - Support Area Guidelines](#)
- [Lab Management](#)
- [Meeting Guidelines](#)
- [Office of Institutional Programs Policy](#)
- [Pace Management Policy](#)
- [Policy/Policy Development Process](#)
- [Productivity Guidelines](#)
- [Recruitment Policy](#)
- [Social Media Guidelines](#)
- [Supervisor/Student Relationship](#)
- [Technology](#)
- [Copyright Guidelines](#)
- [Vendor Contract System Access Policy](#)

i Processes

Processes typically includes documents that describes a repeatably flow of activities. These type of documents would typically be suffixed: *Process, Procedure, Workflow* etc.

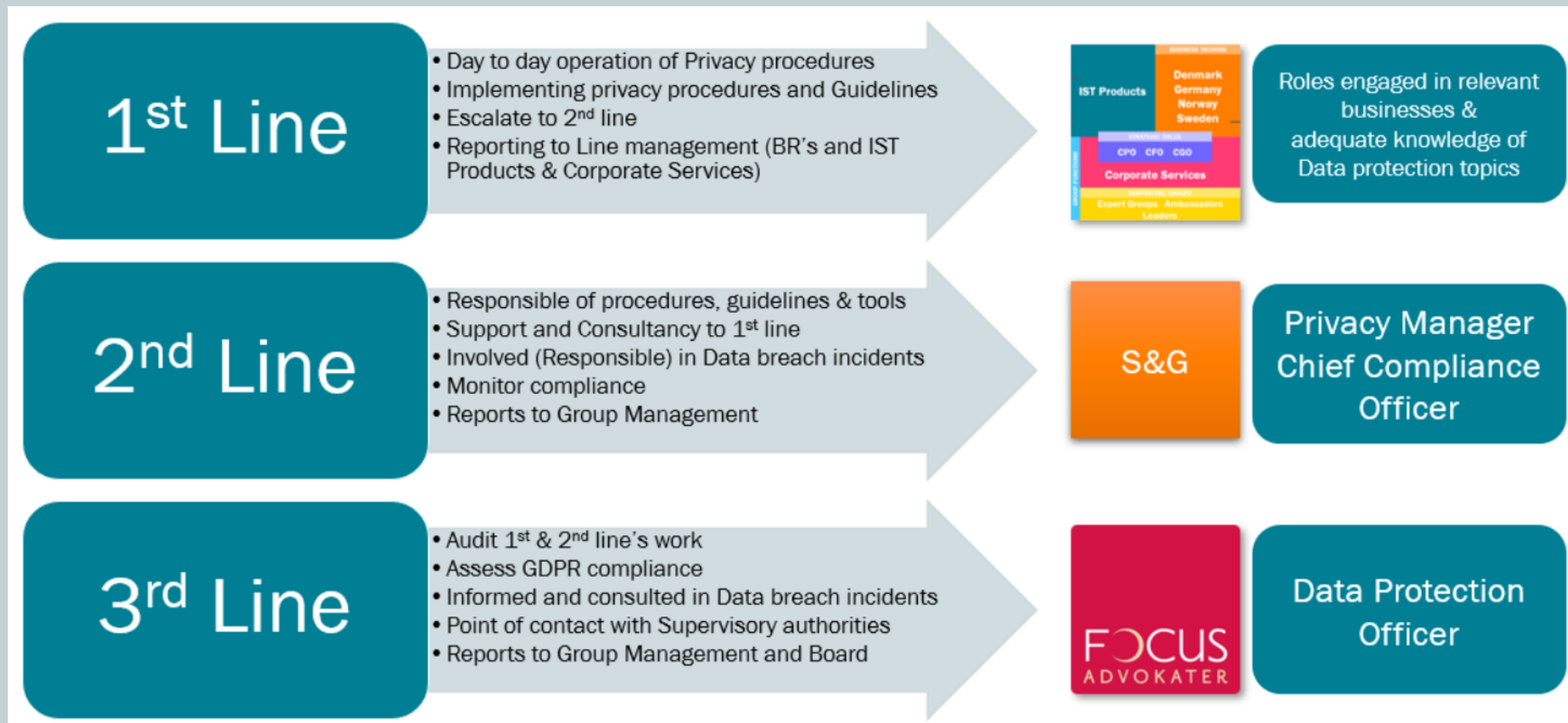
- [illegible]

Templates includes wiki, word, ppt or excel files that serves as templates for the preparations of other documents.

Note that the list below does not contain templates that are tied to a process etc. Such templates are listed in relation to the process.

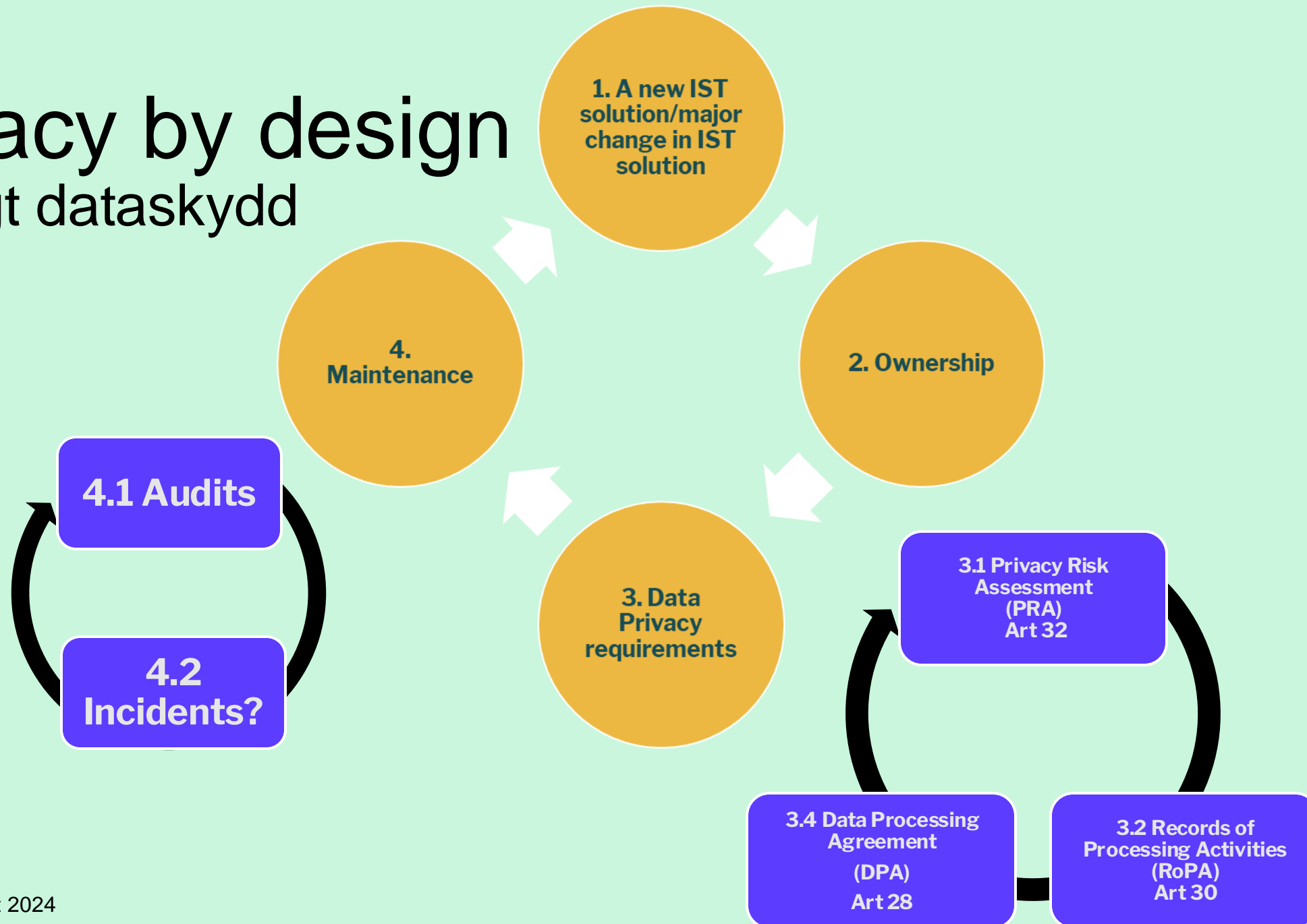
- Agreement Templates
- Corporate Presentation Templates
- Door Sign Templates
- E-mail Signature Templates
- Plain-IST Office Templates
- Privacy Consent Form Templates

Integritetsorganisation



Privacy by design

inbygggt dataskydd



Riskbedömning - Exempel

Riskanalys

Risk No	Risk/Threat Description	Probability	Consequence	Risk Value
10	Guardian gets access to incorrect blog post (system error)	3	3	9
11	Child gets access to blog in guardian phone	4	1	4
12	Blog post needs to be deleted and the author (teacher) is not available	4	3-4	12-16
13	Can be hard to determine who has or has had access to a (possibly deleted) blog post in case of an incident	4	2-3	8-12
14	Incorrect guardian gets access to blog post	3-4	4	12-16
15	Situation changes - blog posts can become sensitive after publishing	3-4	3-4	9-16

Riskhantering

Risk No	Mitigating Description	Prio	Deadline	Owner	Status	Comments	Jira
1, 5, 6, 12, 15	Introduce for publish status of blog posts	Prio 3				File feature, feature critical. Not very complex to implement.	COMMIT-10 - Need for improve publish status functionality for Blogpost 100% COMMIT-124 - Blog - Add publish status and enable in AdminUI
1, 5, 6, 12, 15	Administrator/supervisor who can access and delete all posts	Prio 2				will hopefully be implemented when adding school support.	COMMIT-125 - Investigate how to give administrators access to Communication 100%
1, 5, 6, 12, 15	Automatic deletion from site after specific time	Prio 1				Configurable per customer. Different configurations for chat and blog.	COMMIT-144 - Automatic deletion from site 100% COMMIT-145 - Chat & Blog - Deploy

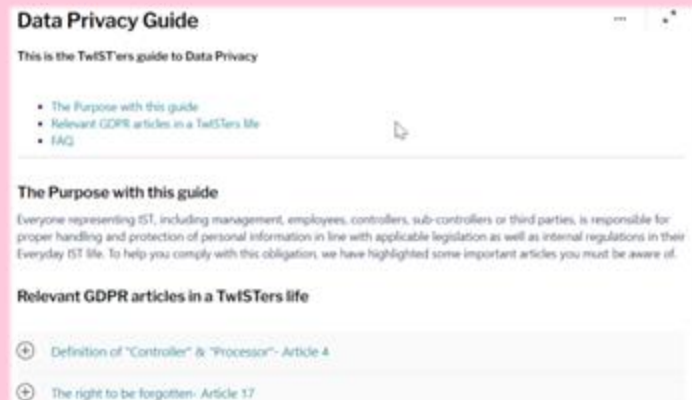
HR

- Bakgrundskontroll
- Sekretessavtal
- Introduktion/avsluta anställning
- Utbildningar



Support

- Personuppgifter i ärenden
- Dokumenterade rutiner
 - Arbete i kundmiljöer
- FAQs, guider

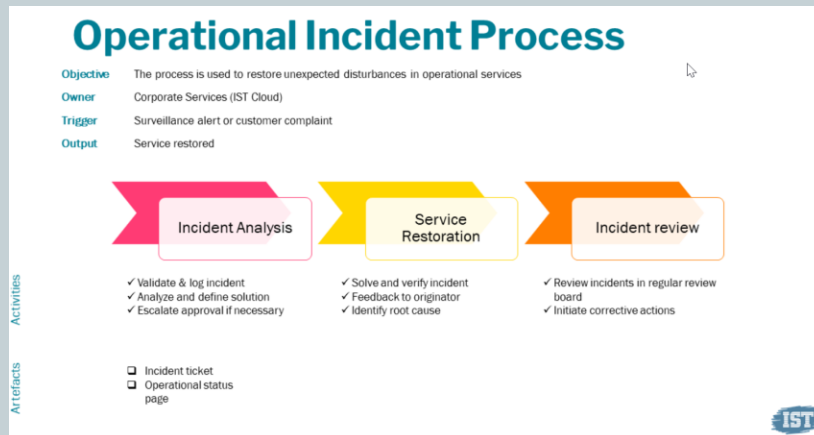
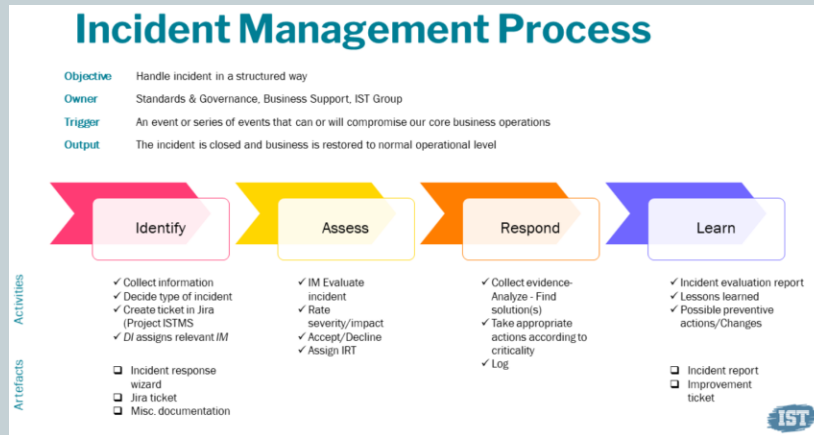


- Incidenthantering



Incidenthantering

- Incidentansvarig



Dokumentation vid Personuppgiftsincident (PUI)

Mall för insamling av information till kund vid personuppgiftsincident



Notifiering till kund

Mall för kundnotifiering vid personuppgiftsincident



Tech & Development

- Kodning
- Test
- Risk – analys och hantering
- Drift - Kontinuitetsplanering



Dataskyddskommitté

Syfte

Initierar och följer upp

Agenda

Årshjul



Lagar – beslut - utbildning



Tack!

Frågor?

Träffa oss på torget!