# INTRODUKTION TIL RECORDS RISK MANAGEMENT MED BAGGRUND I ISO/TR 18128:2014

Norsk Arkivråd, 11. marts 2015

Tine Weirsøe, Scandinavian Information Audit
www.information-audit.dk

## LIDT OM OS…

### Scandinavian Information Audit

- Etableret i 2004
- Specialiseret i records-/document management, arkivering, information governance og informationssikkerhed
- Uafhængig af andre konsuleneter og leverandører, men vi har et godt netværk
- Arbejder i de nordiske lande, Tyskland, Holland, Schweiz, Italien, USA m.fl.
- Vores kunder er virksomheder indenfor:
  - Pharma og lifescience
  - Offshore og energi
  - Transport, shipping og luftfart
  - Fødevarer
  - Den finansielle sektor
  - Statsejede virksomheder og den offentlige sektor
  - Interesseorganisationer

# LIDT OM MIG…

Executive MBA, CBS, 2002
Lead auditor ISO 9001 (ICRA)
Bibliotekar sektion 2, 1985

- 2012- Ekstern lektor og fagansvarlig ved Master i informationsforvaltning og records management, Aalborg Universitet/IVA KU
- 2004- Konsulent, Scandinavia Information Audit
- 1999-2008 Formand for det nationale udvalg bag ISO 30300-serien
- 1993-2004 Novo Nordisk, Records Management Centre. Afdelingsleder fra 1998
- 1993-1994 CBS, business service
- 1987-1992 Børsens Forlag, produktchef og redaktør af Greens
- 1985-1987 Industrifagene (nu DI), datakonsulent



# INDHOLD

- Baggrund for ISO 18128
- Gennemgang af highlights fra standarden
- Værdien af records risk management

## HVORFOR EN STANDARD OM RISIKOVURDERING FOR RECORDS MANAGEMENT?

- Risk management foretages systematisk og er fuldt integreret i for eksempel:
  - Økonomi, finans og investering
  - Informationssikkerhed
  - Projektledelse
  - Luftfart, shipping, transport
  - Lægevidenskab, medicinalindustrien, hospitalsvæsenet
- Risikovurdering i forbindelse af med håndtering af alt det, der har værdi:
  - Menneskeliv
  - Miljø
  - Økonomiske ressourcer og produktionsapparat.

**Har dokumentation, records, arkivalier, information og data værdi?**



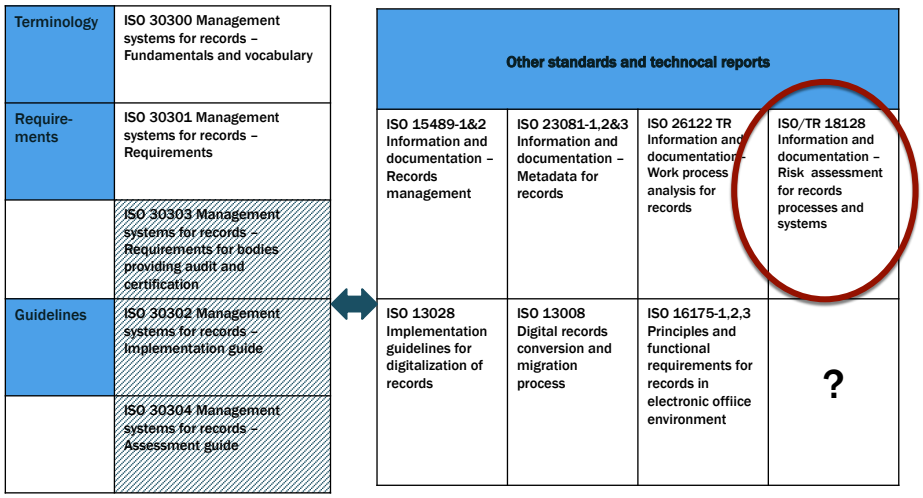
## TERMINOLOGI – HVAD ER RISIKO?

### Risk = effect of uncertainty

- Note 1 to entry: An effect is a deviation from the expected — positive or negative.
- Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
- Note 3 to entry: Risk is often characterized by reference to potential events (ISO Guide 73:2009, 3.5.1.3) and consequences (ISO Guide 73:2009, 3.6.1.3) or a combination of these.

(kilde ISO 18128:2014, fra Iso Guide 73:2009, definition 1.1)

# ISO 30300-SERIEN




# ISO 18128:2014

- Publiceret den 3.marts 2014 – det tog omkring 5 år at udarbejde standarden og få den godkendt i ISO systemet.
- Målgruppen er records managers (records professionals) og andre, der har ansvar for records med at identificere, analysere og minimere risiko
- Det forudsættes, at organisationen allerede har genereret og identificeret records og i det mindste har etableret et minimalt records management system (= records management governance) til kontrol og håndtering af records.

# HENVISNINGER

Referencer

- ISO 30300:2011 Information and documentation – management system for records – Fundamentals and vocabulary
- ISO Guide 73:2009, Risk management – Vocabulary

Bibliography

- ISO 15489-1 & 2
- ISO 23081-1, 2 & 3
- ISO 27001 Information technology – Security techniques
- ISO 31000:2009 Risk management – Principles and guidelines
- IEC 31010:2009 Risk management – Risk assessment techniques



# ISO 18128 - FORMÅL

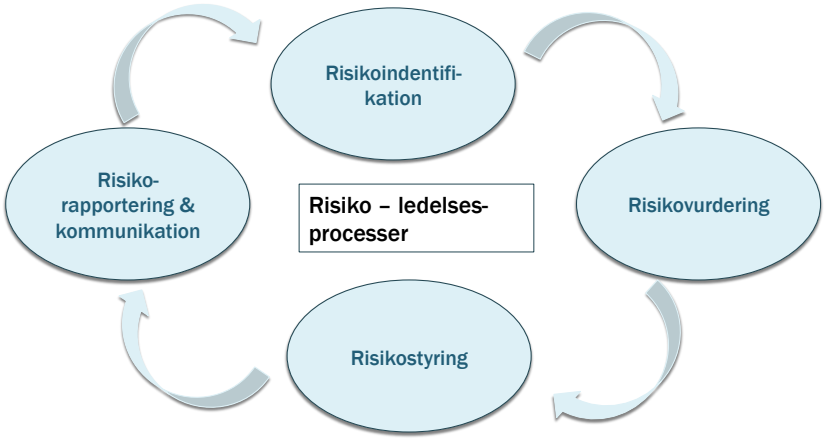
Formålet med ISO 18128 er give en ramme til vurdering af risici ved records processer og systemer, herunder

a) metode til at *identifikation af risici*
b) metode til at *analysere de potentielle følger af utilsigtede hændelser*
c) retningslinjer for at foretage en vurdering af risici, og
d) retningslinjer for *dokumentation af identificerede og vurderede risici* som forberedelse til at minimere effekten (mitigation).

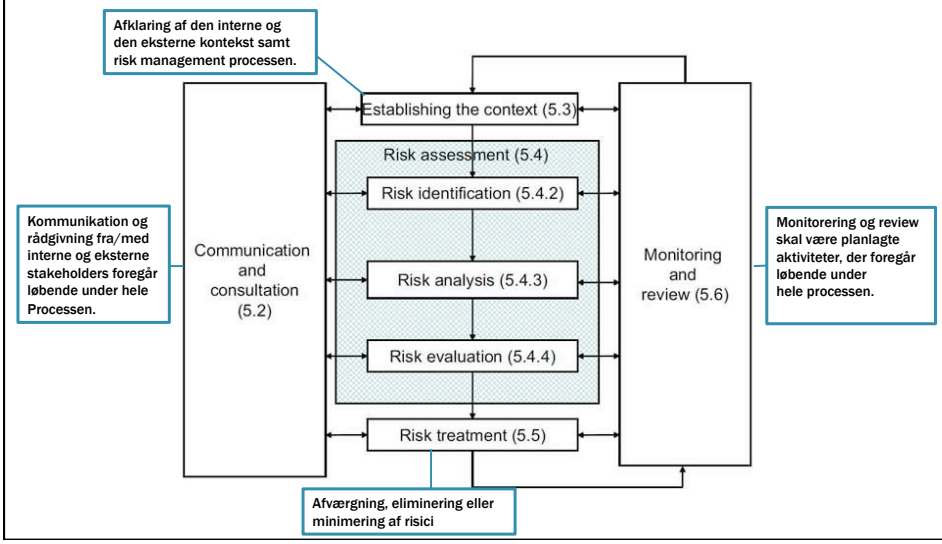
Standarden omhandler ikke de risici, der kan forekomme, hvis en organisation ikke genererer records.

Standarden kan anvendes af alle organisationer – offentlige og private - uanset størrelse, aktiviteter, eller kompleksiteten i funktioner og struktur.

# TRADITIONEL RISIKOLEDELSE OG RISIKOSTYRING

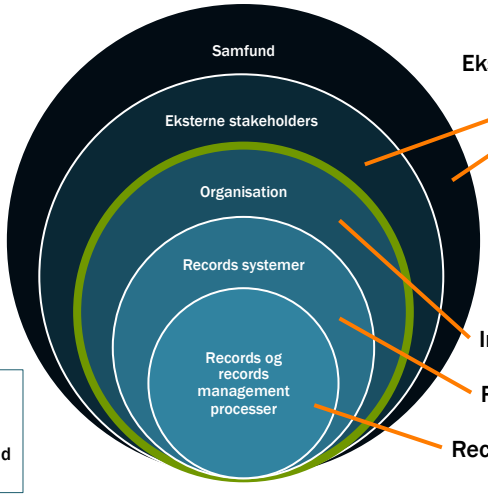



# ISO 18128 RISK MANAGEMENT PROCES (FRA ISO 31000)



# RECORDS MANAGEMENT PROGRAMMET


# STAKEHOLDERS, ORGANISATION OG SYSTEMER - SAMSPIL MED RECORDS OG RECORDS MANAGEMENT PROCESSER




Eksterne risikofaktorer

Interne risikofaktorer

Records systemer

Records processer

ISO 18128, figure 2
The multiple layers of context of an organisation's records and ecords processes

# VURDERING AF RISIKO

Ved vurdering af risiko skal der tages højde for organisationens interne og eksterne kontekst og selve risk management processen.

- Roller og ansvar: Records managers rolle i vurdering af risiko skal specificeres
- Indhold og omfang af risikovurderingsaktiviteter: Grænseflader til andre risk management områder skal afklares for at undgå redundans og konflikter med andre områder og for at sikre en integreret indsats, der inkluderer records.



# CASE: RISKOKRITERIER

Kontraktarkivet indeholder originale kontrakter og er placeret i en kælder med lav grundvandsstand. Der løber desuden kloakrør af ældre dato under loftet i arkivet.

Kriterier for risikovurdering bør være baseret på de juridiske krav og skal indeholde følgende:

a) arten og typer af konsekvenser, der skal omfattes, og hvordan de vil blive målt;
b) den måde, hvorpå sandsynligheder skal fortolkes;
c) hvorledes et risikoniveau, vil blive bestemt,
d) de kriterier, der vil blive fastlagt, når risiko skal formindskes;
e) kriterierne for, hvornår en risiko er acceptabel, og/eller grænseværdier;
f) hvorvidt og hvordan vil kombinationer af risici håndteres.

a) Ødelagte kontrakter. Aftaler og kontraktlige forpligtelser kan ikke afklares. Kontrakter kan ikke opsiges eller fornyes rettidigt. Dyrt at genskabe. Måles ved omkostninger til konservering, konsekvenser for kunder, omdømme, aktiekurs m.m.
b) Sandsynlighed for oversvømmelse i arkivet pga regn eller stigende grundvand.
c) På baggrund af regnmængde og grundvandsstand gennem 10 år samt en VVS-mands vurdering af kloakrørenes tilstand og risiko for lækage.
d) Mindre risiko for oversvømmelse og lækage
e) Når risiko for oversvømmelse og lækage er formindsket med 80%
f) Kombinationer af risici kan være:
   - Vand + råd + svamp

# EKSTERNE RISIKOFAKTORER




# ÆNDRINGER I DEN POLITISK-SAMFUNDSMÆSSIGE KONTEKST

Ændringer i det politiske eller samfundsmæssige miljø, nationalt eller internationalt:

- Ny lovgivning
- Politiske ændringer eller ændring af politisk kurs
- Nye standarder eller ny praksis
- Ændret efterspørgsel efter records management services
- Ændrede forventninger fra omverden (stakeholder expectations)
- Ændringer i omdømme eller tillid til, at organisationen kan levere de forvende ydelser.

# EKSEMPLER PÅ ÆNDRINGER I DEN POLITISK-SAMFUNDSMÆSSIGE KONTEKST

- Ny persondata lovgivning
- Rusland/Ukraine konflikten
- Fra DS 484 til ISO 27001
- Offentlig digitaliseringsstrategi
- Afskaffelse af journalfunktionen i offentlige virksomheder
- Dårlig økonomisk performance
- Manglende leveringssikkerhed, fx overenskomstforhandlinger, der fører til strejker.



# ÆNDRINGER I MAKRO-ØKONOMISKE OG TEKNOLOGISKE RAMMER

Ændringer i makro-økonomiske, forretnings- og branchemæssige forhold og informationsteknologi kan påvirke konkurrence og kundeadfærd. Nedenstående eksterne ændringer vil føre til interne ændringer i en organisation:

- Ændringer i ejerskab eller udbytte, kan påvirke ledelsens prioriteringer, herunder records management
- Ændringer i mål, funktioner og produktionsforhold kan påvirke records management
- Myndigheders stigende eller ændrede aktivitet, kan medføre pres på records management
- Flere retssager eller inspektioner, kan medføre øget efterspørgsel efter records
- Brug af ny teknologi, fx sociale medier, mobile computere og mobile lagring
- Ændringer i organisationens markeder eller kunder.

## EKSEMPLER PÅ ÆNDRINGER I MAKRO-ØKONOMISKE OG TEKNOLOGISKE RAMMER

- Ejerne vælger at trække store beløb ud som udbytte
- Outsourcing af opgaver, fx til Indien
- Konkurrencestyrelsen øger fokus og aktivitet mod en bestemt branche, fx teleselskaber, el-selskaber
- Brug af Facebook til dialog med kunder



## FYSISK MILJØ OG INFRASTRUKTUR

Muligheden for naturkatastrofer eller menneskeskabte katastrofer, der påvirker den generelle drift og sikkerhed er en usikkerheds faktor:

- Nationale eller lokale naturfænomener som jordskælv, orkan/ cyklon, tsunami, oversvømmelse, brand, store storme, eller langvarig tørke
- Krigshandlinger eller terrorisme
- Nedbrud eller ustabil forsyning af el, vand, gas, eksterne informationssystemer, transport, affaldshåndtering, informationsteknologi, transport eller lignende.

## EKSEMPLER PÅ FYSISK MILJØ OG INFRASTRUKTUR, DER KAN ÆNDRE RM

- Kraftig regn den 2. juli 2011 medførte store oversvømmelse i det indre København. Mange arkiver og serverrum blev ødelagt, fx Tivolis arkiv, Kræftens Bekæmpelse



## EKSTERNE SIKKERHEDSTRUSLER

Risikoidentifikation bør omfatte eksterne sikkerhedstrusler med potentiel effekt, der spænder fra skader på lokaler eller ydelseslevering til uautoriseret adgang til systemer, inklusiv records management systemer:

- Uautoriseret ekstern indtrængen i systemer og/eller ændring af records
- Udnyttelse af digital sårbarhed (virus, hacking)
- Fysisk indbrud i arkivet eller IT-drifts lokaler
- Angreb på intranettet, eksterne hjemmesider eller andre systemer
- Hærværk og vandalisme
- Tab af tredjeparts tjenester

# INTERNE RISIKOFAKTORER




# ORGANISATIONSÆNDRINGER

Ledelsesmæssige beslutninger, der påvirker en organisation som for eksempel fusioner, overtagelser og andre opkøb, omstrukturering, nedskæringer, outsourcing, eller insourcing:

- Ændring af ejerskab kan medføre, at records skal udskilles eller overføres samt migrering og konvertering af records og records systemer
- Eventuel fortsat adgang til records for tidligere brugere
- Overtagelse af ansvar og ejerskab af systemer, der ikke er tilstrækkeligt dokumenterede
- Tab af personer med kendskab til records og records management systemer, herunder kendskab til procedurer for brug og ældre records nedarvet gennem organistionsændringer
- Ændringer i vilkår for tredjeparts services
- Nye interne politikker
- Politikker og procedurer, der ikke er opdateret
- Organisationsændringer, der kan påvirke ansvar for records.

# NY TEKNOLOGI

- Teknologiske ændringer, der påvirker interoperabiliteten* mellem systemer
- Kompatibilitet med eksisterende platforme og systemer
- Planlægning og gennemførelse af migrering og konvertering af dokumenter
- Omstrukturering af ansvar og kontrol af DM-processerne
- Inkludering af ny teknologi i eksisterende governance, fx cloud, sociale medier, RFID, GPS.

* Interoperabilitet er produkters, systemers, eller forretningsprocessers evne til at arbejde sammen til at løse en fælles opgave



# RESSOURCER – MENNESKER OG KOMPETENCER

En virksomhed er afhængig af kompetente medarbejdere til udførelse af alle opgaver:

- Antal medarbejdere til at skabe og kontrollere records og til at designe og vedligeholde records systemer
- Bevidsthed om records management politikker og processer
- Topledelsens engagement og støtte til records management
- Bevidsthed om risici i relation til records processer og systemer og topledelsens evne til at tage beslutning, der afbøder alvorlige situationer
- Balancering af forholdet mellem det administrative ansvar for records management og synspunkter fra brugere
- Tab af nøglepersoner med afgørende kompetencer og dybdegående organisatorisk viden
- Forringelse af kompetenceniveauet

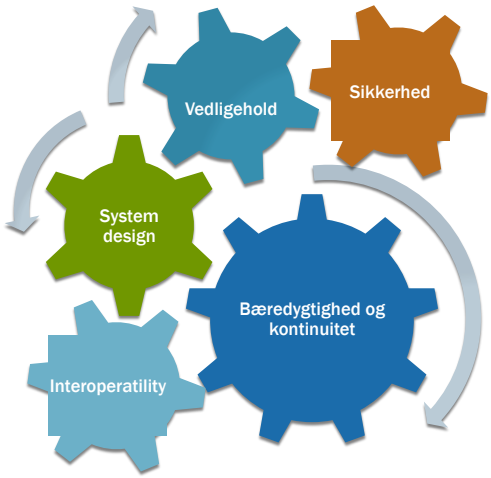
# RESSOURCER – ØKONOMI OG MATERIALER

Finansiering og tilgængelige ressourcer til styring og kontrol af tilstrækkelige records management processer og systemer er påvirket af både den eksterne økonomiske og erhvervsmæssige ramme og af den interne støtte til records management i organisationen

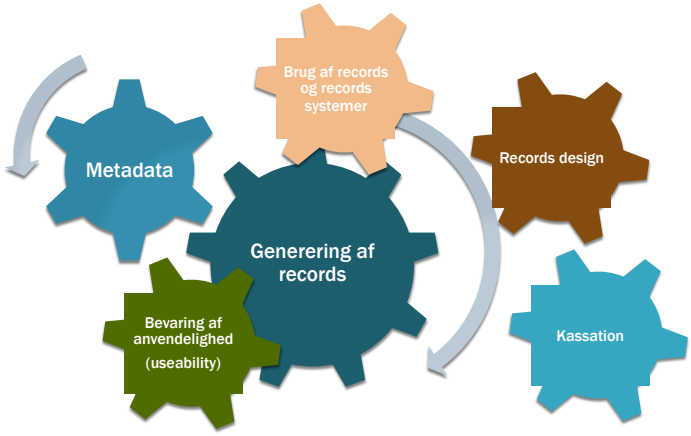
- tilstrækkelige finansielle ressourcer til at opfylde krav til og mål for records management
- tilstrækkelige finansielle ressourcer til at sikre opgradering eller opretholde tilstrækkelige systemer.



# RECORDS SYSTEMER



# RECORDS PROCESSER






# RECORDS PROCESSER

Identifikation af risici i forbindelse med records management processer:

- Generering af records
- Kontrol af de processer, der vedrører håndtering af records, fx
  - Arkivering
  - Påføring af metadata
  - Påføring af retentionperiode
  - Søgning
  - Konvertering
  - Migrering
  - Kassation

# IDENTIFIKATION AF RISICI

**Risici identificeres ved afklaring af potentielle konsekvenser og sandsynligheden for, at det forekommer.**

- **Eksempel på skallering af sandsynligheden:**

| Sandsynligheds score | Forklaring |
|---|---|
| 1 | Sjælden sandsynlighed indtræffer en gang hvert 10 år eller derunder |
| 2 | Lav sandsynlighed sker en gang hver 3. år eller sjældnere |
| 3 | Medium sandsynlighed sker en gang om året |
| 4 | Stor sandsynlighed forekommer mere end en gang om måneden |



# EKSEMPEL PÅ EN RISIKOVURDRING

| Context | System events | Process events | Proba-bility | Minor impact | Moderat impact | Major impact | Severe impact |
|---|---|---|---|---|---|---|---|
| | | Records misclassified, wrong access status | High *Monthly or more* | Recoverable under existing procedures | | | |
| Changes to privacy protection law | | | Medium *Once a year* | | Affects access restrictions to personnel system; flow on to other operations | | |
| | Indexing function of records system fails | | High *Monthly or more* | Recoverable under existing procedures | | | |
| | | Records wrongly identified for destruction | High *Monthly or more* | Recoverable under existing procedures | | | |
| | | Unauthorised access to employee records | Low *Once every 3 years* | | Not recoverable; Apology made to staff | | |
| Fire destroys building holding records systems | | | Rare *Once every 10 years* | | | | Loss of significant records; disruption to operations; loss of public trust |
| | Interruption to power supplies for 8 h | | Low *Once every 3 years* | | | Affects all records systems; one day's transactions lost | |

# EKSEMPEL PÅ EN BESKRIVELSE AF EN RISIKO I "RISK REGISTER"

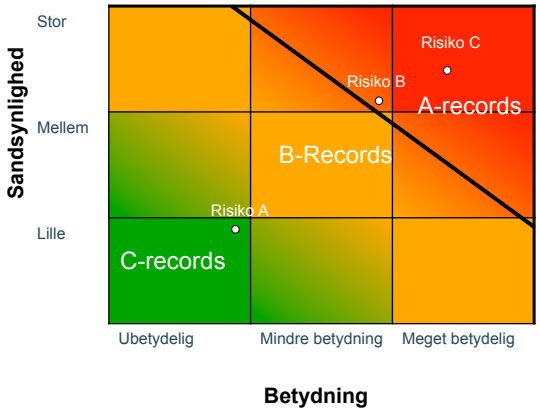
| | |
|---|---|
| *Register fields* | *Item entries* |
| Risk ID | 4 |
| Risk Name | Inability to determine creator of a document. |
| Risk Owner | EDRMS system administrator |
| Date identified | 05-may-2014 |
| Date last updated | 08-may-2014 |
| Description | Unable to find out who the creator of a registered record is |
| Risk manifestation (circumstances within which risk can execute) | Uncertainty about the originating business unit of records |
| Cost if it materialises (monetary or otherwise) | Low |
| Probability | Medium |
| Impact | High |
| Avoidance strategy | Review and fix document templates within EDRMS |
| Target day | 30-may-2014 |
| Action owner/custodian | EDRMS system administrator |
| Cross references related risks | 3, 8, 19 |
| Date of the last assessment | |

# CASE: PRIORITERING AF RECORDS

| Prioritering af records | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Økonomi | | Omdømme | | Sikkerhed | |
| | | Omkostninger ved tab (DKK) | | Omdømmet skades i… | | Manglende håndtering af records efter gældende governance | |
| A-records | Hvis… | 1 milliard | Eller… | International presse | Eller… | Uacceptabel risiko (rød) | Så A |
| B-records | Hvis… | 100 mill. | Eller… | National presse | Eller… | Acceptabel risiko (gul) | Så B |
| C-records | Hvis… | 10 mill. | Eller… | Ingen | Eller… | Acceptabel risiko (grøn) | Så C |

Denne model er ikke inkluderet i ISO 18128

# CASE: PRIORITERING AF RECORDS




Denne model er ikke inkluderet i ISO 18128

# AFSLUTTENDE BEMÆRKNINGER

- ISO 18128:2014 er en ny standard
- Erfaringer – både mine personlige og fra andre records management professionelle – er indtil videre positive
- Metoder fra ISO 18128:2014 er i et par virksomheder integreret i records management programmet og i mindst tre virksomheder integreret i ledelsessystem for informationssikkerhed (ISO 27000)
- Robuste risikovurderinger er sammen med audits/revisioner formentligt vejen frem for at synliggøre records management udfordringerne og risici
- Værdien af records og risici ved dårlig eller manglende records management har altid været svær at synliggøre og bevise – risikovurdering er et skridt på vejen.

# SCANDINAVIAN INFORMATION AUDIT

## Kommende kurser i København

Audit/revison af records management processer, systemer, arkiver og programmer
12. juni 2015

Få overblik over ISO 30300-serien - internationale standarder om information, dokumentation og records management
28. maj 2015

Forretningskompetence for informationsspecialister
2. juni 2015

Risikovurdering for records management, systemer og processer
Værktøjer - metoder - ISO 18128:2014
4. juni 2015

Retention- og kassationspolitikker for records, dokumenter, data, information og viden
15. juni 2015



Tine Weirsøe, Scandinavian Information Audit
Email tw@information-audit.dk – Telefon 70 23 14 04