EU:s Digital Operational Resilience Act, DORA

Nya krav och en praktisk implementation

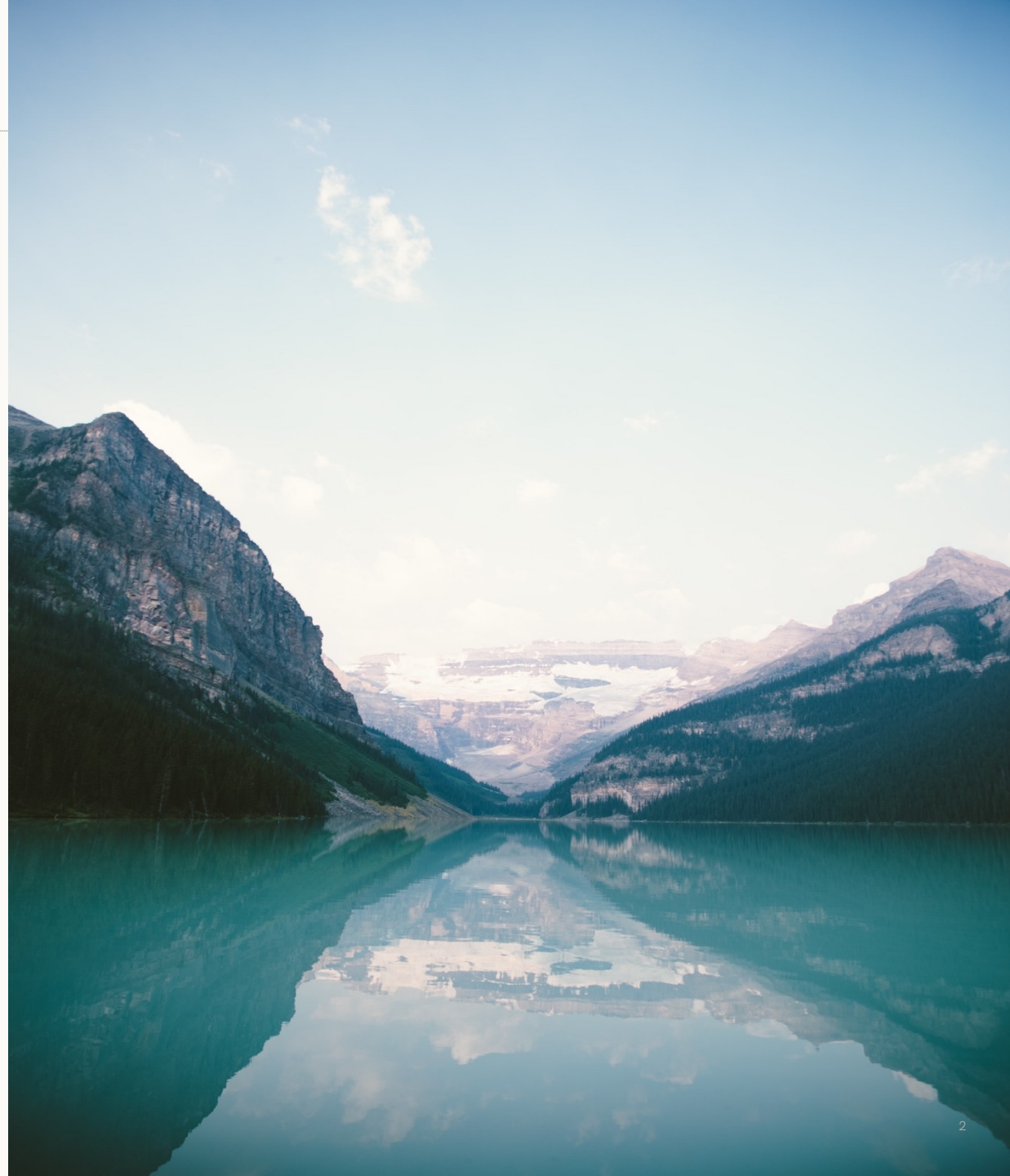
Agenda

Digitalisering och operativ resiliens i finanssektorn är två sidor av samma mynt

01 **DORA regleringen**
- Tidslinje och övergripande krav i DORA

02 **DORA RTS**
- Fördjupande beskrivningar av DORA

03 **Praktisk implementation**
- Hur gör vi då?



Tidslinjen för DORA

DORA är en Förordning inte ett Direktiv

- Förordningar är direkt tillämpliga.
- Direktiv implementeras i nationell lagstiftning.

2022-12-27

DORA formellt accepterat, utkast till RTS:er publiceras löpande

2025-01-17

DORA träder i kraft, inkl. RTS:erna

Regulatorisk status - RTS (Regulatory Technical Standards)?

I princip samma rättsliga status som DORA då de fastslås av EU kommissionen och förtydligar eller tolkar DORA.

Syftet med DORA är att säkerställa ett instituts digitala operativa motståndskraft

Vad är det?

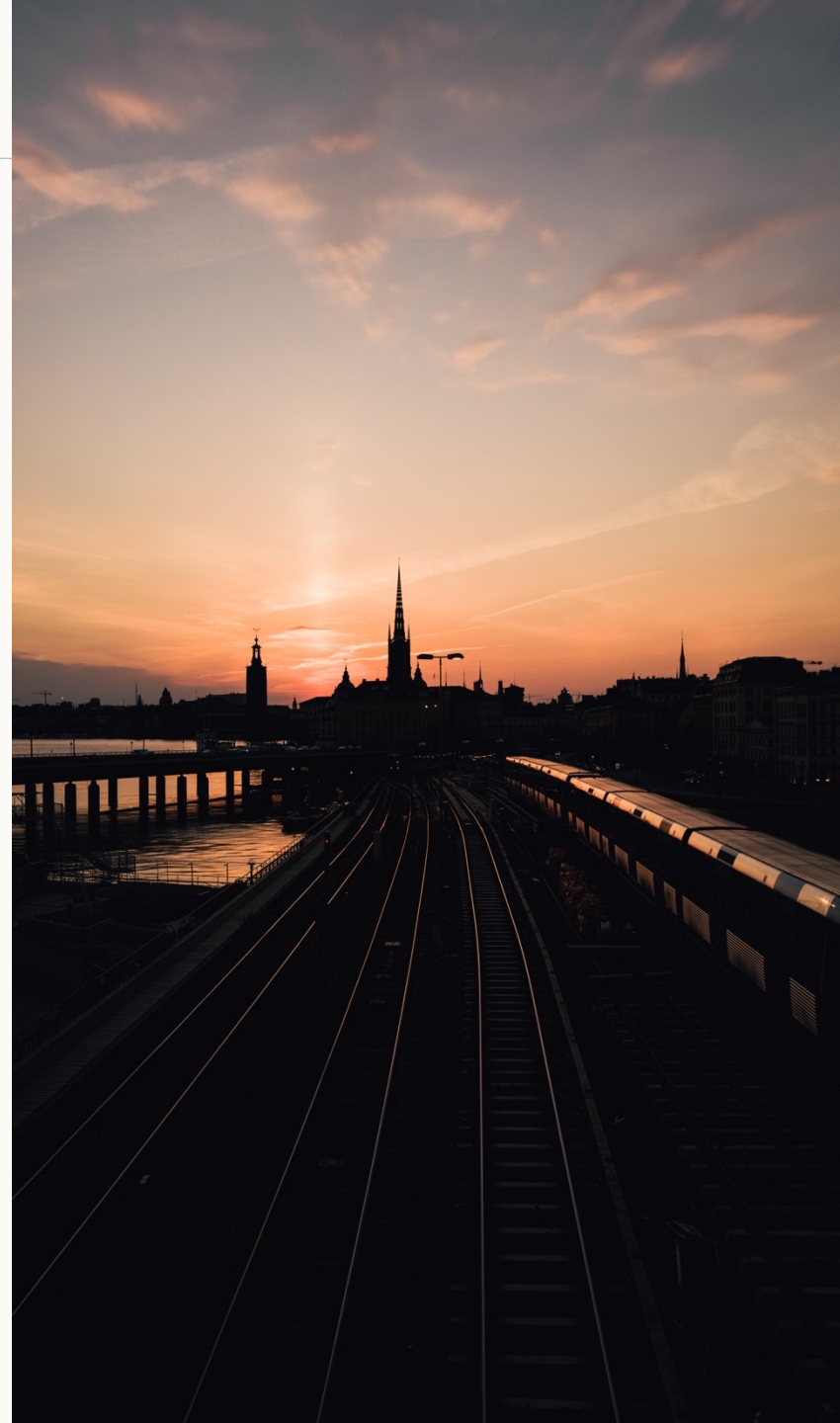
Digital Operativ Motståndskraft

Beskrivning

- Digital Operativ Motståndskraft: en finansiell enhets förmåga att bygga upp, säkerställa och se över sin operativa integritet ur ett tekniskt perspektiv genom att, direkt eller indirekt, med användning av tjänster från IKT-tredjepartsleverantörer, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell enhet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet.

Eller:

- Ett institut och hela finanssektorns förmåga att identifiera och förbereda sig för, reagera och anpassa sig till, återhämta sig och lära sig av störningar eller avbrott i verksamheten.



DORA är uppdelad i 6 övergripande regleringsområden

Detaljnivån av DORA är omfattande

01	02	03	04	05	06
Styrning och organisation	IKT-riskhantering	IKT-relaterad incident-hantering	Testning av digitala operativa motstånds-kraften	Hantering av IKT tredjeparts-risker	Informations-utbyte

2024-01-17

Första omgången

- **Artikel 15. ytterligare harmonisering av verktyg, metoder, processer och policyer för IKT-riskhantering**
- Artikel 16. Simplified ICT RMF
- Artikel 18. Klassificering av ICT incidenter
- Artikel 28. Krav inom utkontraktering
- Artikel 28 (ITS) – registrering av information (outsourcing)

2024-07-17

Andra omgången

- Artikel 20. Rapporteringsmallar
- Artikel 20 (ITS) standardiserade mallar
- Artikel 26. TLPT tester
- Artikel 30. Huvudavtalsklausuler vid utkontraktering av ICT
- Artikel 41.Krav på tillsynsmyndigheten

2025-01-17

Tillämpningsdatum

Proportionaliteten i RTSerna?

Proportionalitet i RTS

1 Specificering

2 Tydlighet

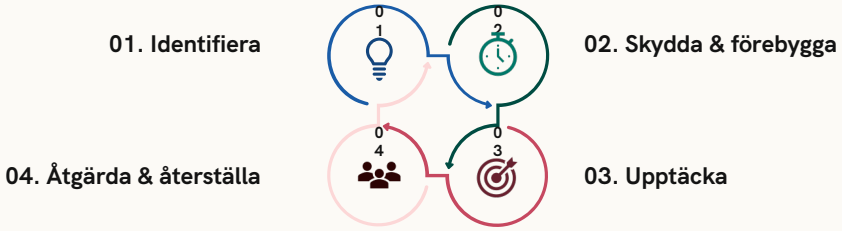
- Innehåller minimi- och skallkrav
- Omvänd proportionalitet för bolag som omfattas!

IKT riskramverket

- Ytterligare harmonisering av verktyg, metoder, processer och policyer för IKT-riskhantering som är en detaljering av Artikel 15 i DORA

Övergripande slutsatser:

- RTS:en fokuserar främst på informationssäkerhet och omfattar krav på innehåll i ett ledningssystem för informationssäkerhet samt interna kontroller för uppföljning av kraven
- RTS:en är detaljrik - SKALLKRAV
- RTS kraven inspirerade av EBA/EIOPA IKT reglering.



Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Informationssäkerhetspolicy

- Kopplar ihop institutens Informationssäkerhetsmålsättning med Strategin för Digital Operativa Motståndskraft
- Kräver en informationssäkerhetspolicy med tillhörande internkontrollaktiviteter

Kontrollfunktionen

- Rapportering och rådgivning till styrelsen
- Styra och övervaka institutets ICT risker
- Definiera IKT- och informationssäkerhetsmålsättningarna
- Utveckla och övervaka effektiviteten av IKT säkerhetsutbildningar och andra kampanjer för medvetandegörande, samt utbildning inom digital operativ motståndskraft
- Måste vara oberoende från funktionen/funktionerna som ansvar för IKT utveckling, styrning, förändringshantering och drift (dvs IT-avdelningen)

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Ramverket för IKT riskhantering (policy):

- Omfattar policy och styrande dokument som säkrar nätverk, intrångsskydd och dataintegritet.
- Fastställer godkända risktoleransnivåer och åtgärder för riskminskning.
- Kräver regelbunden riskanalys och övervakning av IKT-förändringar.

Tillgångsregister:

- Övervakar och hanterar IKT-tillgångarnas livscykler och klassificeringar.
- Innehåller unika identifieringar, geografisk placering, ägarskap och kontinuitetskrav.
- Dokumenterar exponering mot externa nätverk och beroenden mellan IKT-tillgångar och affärsfunktioner.

Ytterligare harmonisering

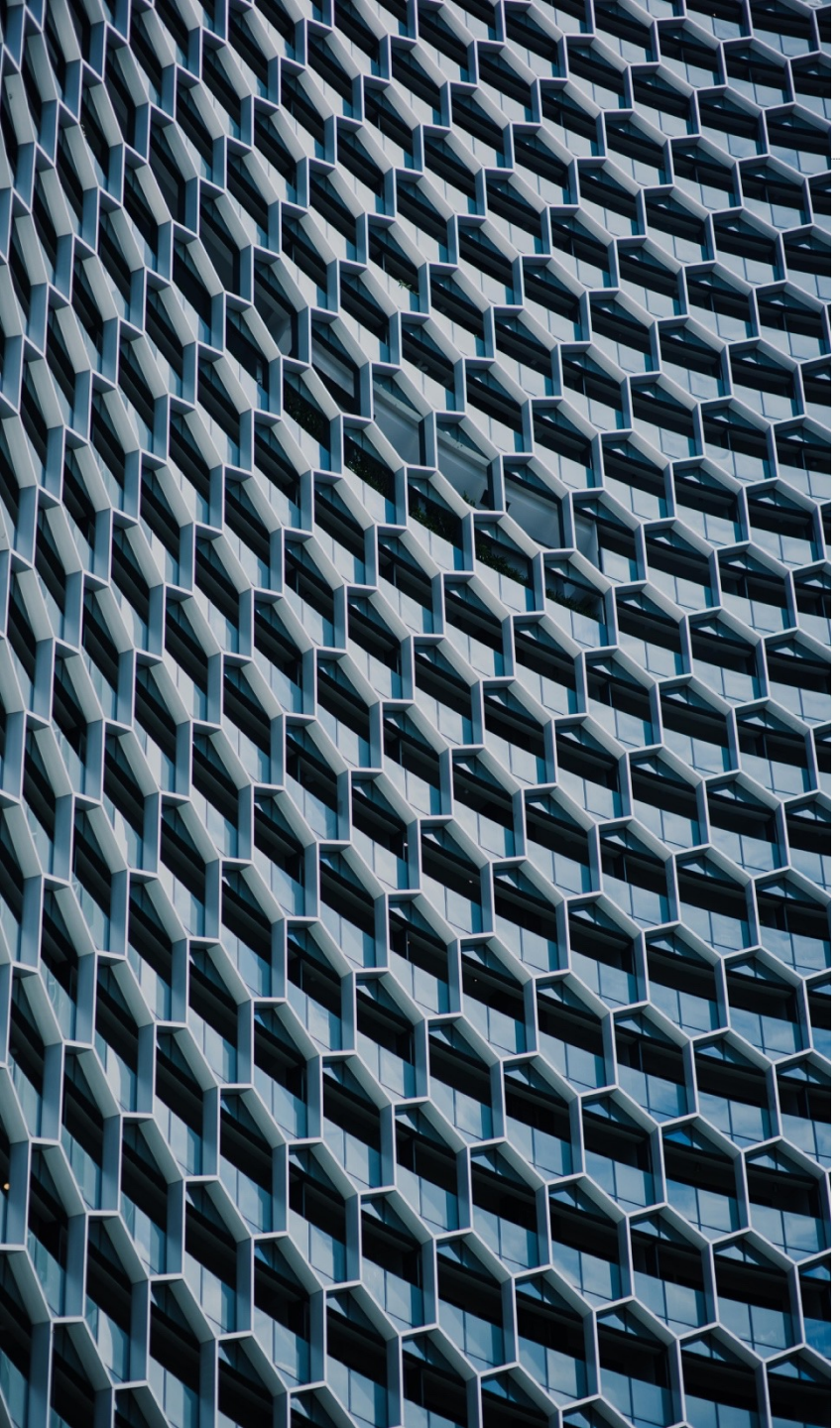
Verktyg, metoder, processer och policyer för IKT-riskhantering

Kryptering och kryptografiska kontroller:

- Krav på kryptering av data i vila, under transport och när data används, baserat på informationsklassificering och kritikalitetsbedömningar.
- Krav på kryptering av interna nätverk, kopplingar till externa parter och nyckelhantering.

IKT drift:

- Rutiner för säker installation, underhåll och konfiguration av IKT-tillgångar, inklusive dokumentation av IKT-processer.
- Interna kontroller för säkerhetskopiering, schemalagda arbeten, system- och revisionsloggar, segregering av produktionsmiljöer, felhantering, och återställning.
- Automatisk sårbarhetscanning, patch-hantering, och övervakning av mjukvarupaket.



Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Data och systemsäkerhet

- Behörighetshantering baserat på informationsklassificering.
- Säkerhetskonfiguration för IKT-tillgångar med säker baskonfiguration. Kontroller för att endast godkänd mjukvara används.
- Användning av endast godkända och användarskyddade klienter som är centralt administrerade för att säkerställa dataskydd och möjlig radering av data som inte längre används.

Loggning

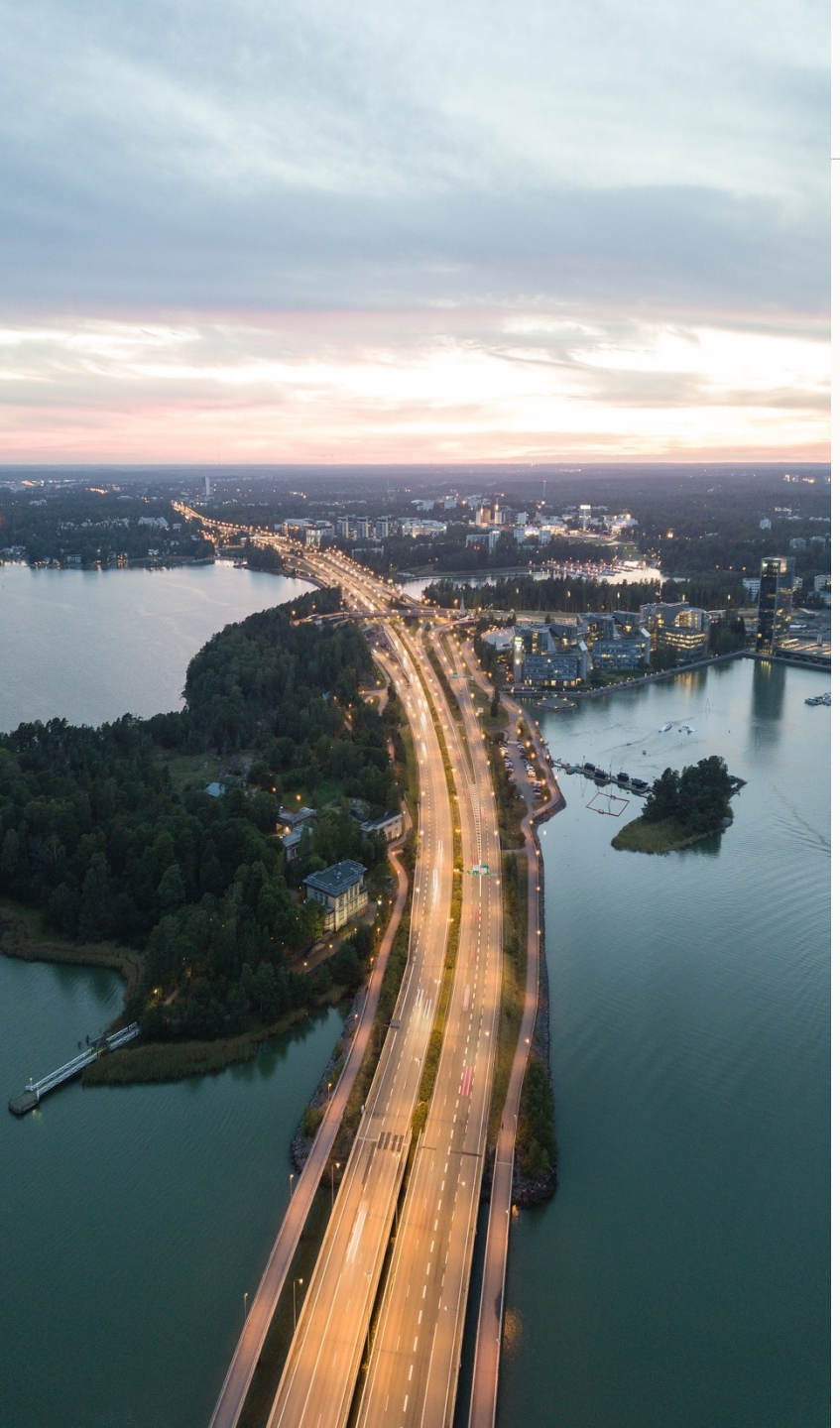
- Interna krav på vilka händelser som ska loggas, lagringstid för loggar, loggdatabehandling och analysförmåga. Kraven gäller även tredjepartsleverantörer.
- Förmåga att automatiskt generera larm vid onormala aktiviteter för kritiska eller viktiga funktioner baserat på fördefinierade regler.
- Loggning av logisk och fysisk åtkomstkontroll, identitetshantering, kapacitetshantering, förändringshantering, IKT-drift och systemaktiviteter samt nätverkstrafik. Proaktiv logganalys med automatisk identifiering av onormala förhållanden eller beteenden.

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Nätverkssäkerhet:

- Segregerade och krypterade nätverk baserat på klassning och kritikalitet.
- Förmåga att isolera och stänga av nätverksdelar.
- Kartläggning och avtal med utrustningsleverantörer.
- Separat administrationsnätverk för systemadministration.
- Åtkomstkontroll och förändringshantering.
- Årlig säkerhetsgenomgång och grundkonfiguration för nätverkskomponenter.



Verktyg, metoder, processer och policyer för IKT-riskhantering

IKT projektledning

- Projektledningsmodellen ska omfatta:
  - Projektmål.
  - Styrningen av projektet, inkl. roller och ansvar.
  - Planering av projektet, tidsramar och steg inom projektet.
  - Riskanalyser av projektet.
  - Projektmilstolpar.
  - Förändringshanteringsrutin för projektet.
  - Testning av krav, inklusive säkerhetskrav samt godkännandeprocess för produktionssättning av projektet.

- För projekt som omfattar Kritiska eller Viktiga funktioner ska alla risker samt status av projektet rapporteras till styrelsen, löpande och när behov uppstår.

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Upphandling, utveckling och underhåll av IKT-system

- Säkerhetskrav inom säkerhet på upphandling, utveckling och underhåll av IKT-system och omfattar identifikation av funktionella och icke-funktionella krav.
- Krav ska finnas på hantera risken för ofrivillig ändring eller manipulation av IKT-system.
- Krav på testning (inkl. säkerhetstestning) innan produktionssättning av köpta eller nyutvecklade tjänster och efter underhåll.
- Integritets och konfidentialitetskontroller för data i icke-produktionssystem (utvecklingsmiljön och testmiljön). Visst användande av produktionsdata är tillåtet vid testning men är reglerat .

IKT förändringshantering

- IKT förändringshantering omfattar: (1) mjukvara, (2) hårdvara, (3) firmware, (4) system och (5) säkerhetsparametrar/konfigurationer.
- Det finns omfattande krav i RTS:en på innehåll av förändringshanteringsrutinen.

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Fysisk och miljörelaterad säkerhet

- Skydd av lokaler, data center och andra känsliga fysiska områden där IKT-tillgångar eller system lagras.
- Skyddet ska omfatta både interna och externa skydd med utökad fokus på IKT-tillgångar utan tillsyn.
- Krav på ”clear desk” och ”clear screen” policy.

IKT och informationssäkerhetsbaserade medvetandegörande kampanjer och utbildning

- Krav på specifika IKT säkerhetsbaserade medvetandegörande kampanjer och formella utbildningar inom digital operativ motståndskraft.
- Minst årliga medvetengörande kampanjer och formella utbildningar.

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Personsäkerhet och behörighetshantering

- I personalpolicyn ska ansvar för informationssäkerhet framgå.
- Alla anställda och tredjepartsleverantörer ska vara medvetna om innehållet i informationssäkerhetspolicyn (och underliggande ledningssystem).
- Vara medvetna om rapporteringskanaler avseende detektering av onormal aktiviteter.
- Vid avslut av anställning ska alla IKT-tillgångar och information lämnas tillbaka till det finansiella institutet.

Behörighetskontroll

- Behörighetskontroller ska vara definierad efter principerna 1) Need-to-know, 2) Need-to-use, och 3) least-privilege. Gäller även fysisk behörigheter.
- Analys avseende uppdelning av arbetsuppgifter ska genomföras för att begränsa otillåten tillgång till information och säkerställa ”toxiska” behörighetskombinationer.
- Begränsa så långt som möjligt användandet av generiska och delade konton, där användare ska kunna identifieras och handlingar i IKT-system spåras (loggas).
- Behörighetsrutiner att tilldela, ändra och ta bort behörigheter (inkl. administratörskonton).

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

IKT-relaterade incident detektering och hantering

- Förmågan att detektera onormal förhållanden och incidenter ska minst omfatta:
  - Beskrivning av den IKT-relaterade incidenthanteringsprocess inkl. förteckning över både intern personal och externa personal som är direkt involverade i incidenthanteringsprocessen med beskrivning av roller och ansvar.
  - Tekniska, organisatoriska och operationella mekanismer som stödjer incidenthanteringsprocessen för att snabbt kunna upptäcka onormal förhållanden och beteenden och för att kunna säkra spår och bevis för en IKT-baserad incident. Denna förmåga ska omfatta automatiserade alarm av onormal förhållanden eller beteenden (för Kritiska eller Viktiga funktioner).
  - Incidentförmågan ska omfatta:
    - (1) misstankar om illvillig aktiviteter inom IKT-system eller nätverk,
    - (2) detektering av data förlust,
    - (3) misstankar om felaktigheter inom transaktioner eller IKT-drift,
    - (4) vid frånfall (oväntade avbrott) av IKT-system eller nätverk,
    - (5) problem som rapporterats av användare, och
    - (6) incident notifieringar från tredjepartsleverantörer.
  - Dessa larm ska hanteras inom en på förhand definierad tidsrymd (expected recovery time).

Ytterligare harmonisering

Verktyg, metoder, processer och policyer för IKT-riskhantering

Kontinuitetshantering

- Styrdokument ska definiera målsättningen med IKT kontinuitetshantering för IKT-tillgångar, hur IKT kontinuitetshanteringen interagerar med den övergripande affärskontinuitetsplanen, och utgå från resultatet av påverkansanalyser (BIA)
- IKT kontinuitetsplanerna ska består av specifika IKT kontinuitetsplaner för allvarliga störningar eller kriser ur ett affärsperspektiv, baserat på RTO och RPO av Kritiska eller Viktiga funktioner genom riskbaserad ansats
- Krav avseende testning av kontinuitetsplaner omfattar att säkerställa att institutet kan upprätthålla kärnaffären tills dess att kritisk affärsverksamhet är återställd
- Planerna ska minst revideras årligen och resultatet (inkl. eventuella brister) ska rapporteras till styrelsen

Verktyg, metoder, processer och policyer för IKT-riskhantering

IKT återställningsplaner

- Ska vara dokumenterade och utgår från återställningsmålsättning för kritiska IKT-system och tjänster. Planerna ska innehålla tydliga roller och ansvar och omfatta både kortsiktiga och långsiktiga återställningsaktiviteter (flera olika alternativ ska finnas om den primära återställningsplanen inte är genomförbara ur ett kortsiktigt perspektiv).

- Planerna ska uppdateras vid incidenter, tester, nyupptäckta risker och hot och förändrade återställningsmål. Planerna ska identifiera relevanta scenarier.

- Det ska finnas kontinuitetsförmåga för att hantera fel eller bortfall av IKT tredjepartsleverantörer.

Krav avseende Kritiska eller Viktiga funktioner

Förhållandet till tredjepartsleverantörer inom IKT

Kritiska eller Viktig funktion

Beskrivning

Kritisk eller viktig funktion: en funktion vars störning väsentligt skulle försämra en finansiell enhets finansiella resultat, eller sundheten eller kontinuiteten av dess tjänster och verksamheter, eller om denna funktion upphörde, uppvisade brister eller misslyckades med utförandet av denna funktion väsentligt skulle försämra en finansiell enhets fortsatta uppfyllande av villkoren och skyldigheterna baserat på sina tillstånd eller med sina andra skyldigheter enligt tillämplig lagstiftning om finansiella tjänster

Eller enklare uttryckt:

En funktion vars bortfall skulle äventyra ett instituts finansiellt resultat, operativa förmåga eller förmåga att efterleva lagar och regler (inkluisive tillsånd enligt Finansinspektionen)

Krav avseende Kritiska eller Viktiga funktioner

Förhållandet till tredjepartsleverantörer inom IKT

Krav för IKT-Outsourcing och Policy

- RTS-krav som påverkar konsoliderade situationer.
- Krav på en multi-leverantörsstrategi.
- Policy för reglering av IKT-outsourcing, inklusive utvärderingskriterier.
- Omfattande planeringsfas före outsourcing:
  - Inkluderar riskanalys, Due Diligence och godkännandeprocess.
  - Täcker operativa, juridiska, IKT, säkerhets-, GDPR- och koncentrationsrisker, med mera.
  - Bedömer teknisk kapacitet, ekonomisk styrka, informationssäkerhet med mera.
  - Löpande analys av intressekonflikter.

Krav avseende Kritiska eller Viktiga funktioner

Förhållandet till tredjepartsleverantörer inom IKT

Krav och Åtgärder för Tredjepartsleverantörshantering

- Man kan inte förlita sig uteslutande på tredjepartsintyg utan måste genomföra egna revisioner (omfattande krav kravställer på tredjepartsintyg).
- Tredjepartsleverantörer ska rapportera på definierade KRIer och interna kontroller. Omfattande rapportering från tredjepartsleverantören till institutet behöver upprättas
- Institut behöver löpande övervaka tredjepartsleverantörerna avseende regulatorisk efterlevnad, informationssäkerhet och kontinuitetshantering.
- Avslutskriterier (termination phase) och exit-strategier (som ska testas).

Praktisk DORA implementation?

Förslag till struktur för praktisk implementation

Gap- eller nulägesanalys (inkl. eventuell mognadsanalys)

Anpassad handlingsplan

Organisation

Rapportering till styrelsen

Anpassning av riskramverket

Utveckling av ett ledningssystem för informationssäkerhet inkl. **interna kontroller**

IKT-baserad incidenthanteringsprocess

IKT testramverk samt integration i IT-utveckling och inköpsprocess

Outsourcing

- Tredjepartsleverantörer
- Due Diligence nuvarande leverantörer
- Omförhandling av krav
- Rutiner för övervakning och kontroll
- On-boarding av nya leverantörer

Rutiner för efterlevnad (inkl. insyn och kontroll av tredjepartsleverantörer)

Sammanfattning av DORA

Viktigaste punkterna från DORA:s artikel 15

01

Sense-of-urgency

Oavsett tillståndskategori så visar RTS:erna på en ambitionsnivå vi tidigare inte sett.

Det är mycket som behöver implementeras och mogna i verksamheten för att kunna konstatera en rimligt nivå av efterlevnad av DORA

02

Kraven är omfattande

Artikel 15 i DORA är lite av en ”Pandoras ask” och omfattar detaljerad SKALL kravställning avseende informationssäkerhets förmågor.

Fundamentalt är:

- Processkartläggning
- Kravställning i styrande dokument
- Internkontrollramverk
- Dokumentation av testning

03

Utkontraktering av Kritiska eller Viktiga funktioner

Omfattande tillkommande krav finns för utkontrakteringsleverantörer som klassificeras som Kritiska eller Viktiga.
Omfattande rapportering från leverantörerna måste ske, och kontroller från instituten.

04

OUTSOURCING

Outsourcing omfattar de krav som finns i EBA/EIOPA regelverken men DORA går längre då DORA kräver kategorisering i flera led, dvs direkta tredjepart-leverantörer men även underleverantörer i flera led som ska dokumenteras i outsourcing-registret

Tack för oss

Fredrik Ohlsson
Managing Director, FCG

072-179 49 51

fredrik.ohlsson@fcg.se

Filip Fabri
Senior Associate, FCG

072-161 77 27

filip.fabri@fcg.se


FCG