Vilka krav ställer DORA på organisationer?

Johan Lindfors, den 14 maj

BG Institute
EN DEL AV BLENDOW GROUP

Välkommen!

Johan arbetar inom PwC:s rådgivningsverksamhet för risk- och regelverk inom den finansiella sektorn. Han är ansvarig och involverad som expert i ett flertal DORA-projekt för PwC:s kunder inom finans och försäkring.

Johan har gedigen erfarenhet av att implementera regelverk med fokus på krav som rör företagsstyrning och hantering av risker, inklusive IT- och informationssäkerhetsrisker.

Utöver PwC har Johan också en bakgrund som bolagsjurist inom SEB.

BG Institute
EN DEL AV BLENDOW GROUP

Agenda

- Vad är DORA och vilka omfattas av kraven?
- Vad behöver finansiella företag och dess IT-leverantörer göra för att efterleva DORA?
- Några praktiska medskick och frågestund

BG Institute
EN DEL AV BLENDOW GROUP

Pass I
Vad är DORA och vilka omfattas?

BG Institute
EN DEL AV BLENDOW GROUP

Vad är ”Digital Operational Resilience Act”?

- Heltäckande **EU-förordning** om digital operationell motståndskraft på **finansmarknaden** inom EU

- **Enhetligt angreppssätt** mot **cybersäkerhet och motståndskraft** genom regler om riskhantering, incidenthantering och testning av IT-system

- **Gäller de flesta** s.k. ”finansiella entiteter” men med **inbyggda proportionalitetsmekanismer** baserade på storlek, risk och komplexitet

- **DORA gäller från januari 2025** - mer detaljerade tekniska standarder utvecklas under den 24 månader långa implementeringsperioden (2023-2024)

IKT är informations- och kommunikationsteknik

Nästan alla bolag under tillsyn av Finansinspektionen behöver tillämpa DORA

- Kreditinstitut
- Betalningsinstitut
- Leverantörer av kontoinformationstjänster
- Institut för elektroniska pengar
- Värdepappersföretag
- Leverantörer av kryptotillgångstjänster
- Värdepapperscentraler
- Centrala motparter
- Handelsplatser
- Transaktionsregister
- AIF-förvaltare
- Förvaltningsbolag
- Leverantörer av datarapporteringstjänster
- (Åter)försäkringsföretag
- (Åter)försäkringsförmedlare
- Tjänstepensionsinstitut
- Kreditvärderingsinstitut
- Administratörer av kritiska benchmarks
- Leverantörer av gräsrotsfinansieringstjänster
- Värdepapperiseringsregister

Tredjepartsleverantörer av IKT-tjänster omfattas av ett särskilt regelverk i DORA

Givet den stora träffytan är proportionalitet och ett riskbaserat arbetssätt nyckelfrågor

- Det spelar roll om du är ett **mikro, små- eller medelstort företag** enligt EU:s definition
- Vissa aktörer är **helt undantagna** t ex AIF-förvaltare som inte behöver tillstånd eller mindre försäkringsförmedlare
- Högre kravställning på bolagets så kallade **kritiska eller viktiga funktioner**
- **Hotbildsstyrda penetrationstester** (TLPT) baserade på TIBER-ramverket var tredje år för de allra största aktörerna
- Små bolag har ofta - i allt väsentligt - sin **IT-verksamhet utkontrakterad** – naturligt att lägga störst vikt vid hantering av leverantörsrisk

Pass II
Vad behöver finansiella företag och dess IT-leverantörer göra för att efterleva DORA?

BG Institute
EN DEL AV BLENDOW GROUP

DORA:s fyra obligatoriska pelare

- IT-riskhantering
- Incidenthantering för IT
- Testning av IT-system
- Hantering av IT-leverantörsrisk

Intern styrning och kontroll över IT-risker behöver i många fall förstärkas

Styrelse och företagsledning ska styra och övervaka arbetet med digital motståndskraft

Fastställa och övervaka den övergripande **strategin, risktoleransnivån** och **riskramverket** för IT-risker

Säkerställa lämpliga **roller, ansvar och rapportering** för IKT-risk – inklusive oberoende kontrollfunktion

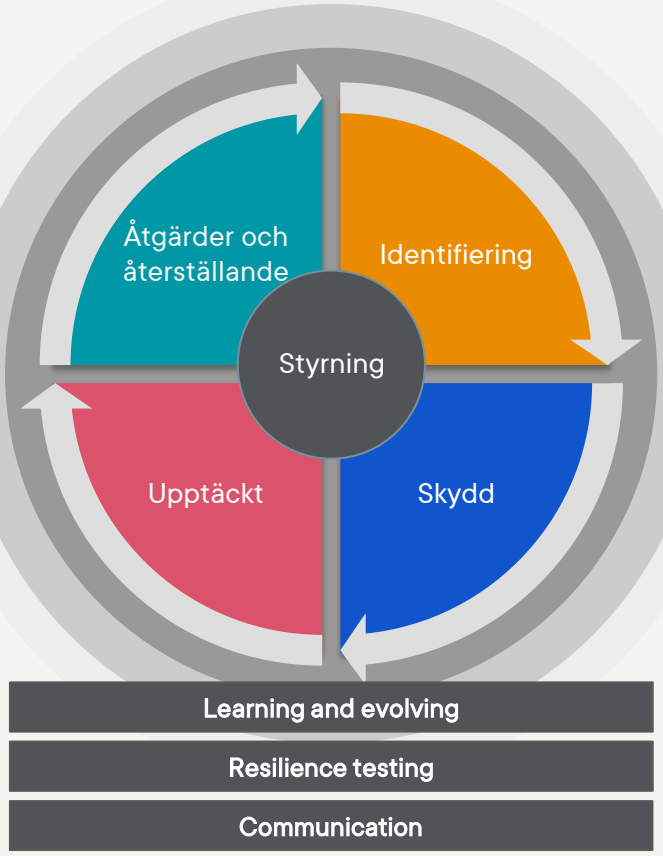
Anta och regelbundet se över **styrdokument** avseende informationssäkerhet, IT-säkerhet och IT-leverantörer

Anslå **lämplig budget** för bolagets behov av digital motståndskraft

Upprätthålla tillräckliga och aktuella **kunskaper och färdigheter** för att förstå och bedöma IKT-risk

Bolagen behöver ha en omfattande strategi, system och process för att hantera IT-risker i sin verksamhet

IT-riskhantering | Incidenthantering | Testning av IT-system | Hantering av IT-leverantörsrisk



Art. 5 Styrning och organisation
Korrekt tone-at-the-top

Art. 6 IKT-riskhanteringsram
En i verksamheten integrerad strategi för digital operativ motståndskraft

Art. 7 IKT-system-, protokoll- och verktyg
Lämpliga, tillförlitliga, tillräckliga och motståndskraftiga

Art. 8 Identifiering
Identifiera risker och skapa en förteckning över funktioner, processer, tillgångar, leverantörer och dess beroenden

Art. 9 Skydd och förebyggande
Förebygg med t ex nätverkssäkerhet, behörighetskontroller och strukturerad förändringshantering

Art. 10 Upptäckt
Upptäck och varna för anomalier – testa upptäcktsförmåga

Art. 11 Åtgärder och återställande
Kontinuitetsplaner, återställningsplaner och konsekvensbedömningar

Art. 12 Säkerhetskopiering m.m.
Metoder för återskapande och återställning

Art. 13 Lärande och utveckling
Var informerad om sårbarheter och cyberhot, lär och utveckla proaktivt och från incidenter

Art. 14 Kommunikation
Kriskommunikationsplaner – internt och för kunder

BG Institute
EN DEL AV BLENDOW GROUP

Allvarliga IT-incidenter ska rapporteras till Finansinspektionen

IT-riskhantering | **Incidenthantering** | Testning av IT-system | Hantering av IT-leverantörsrisk

DORA kräver att finansiella enheter upprättar och implementerar en incidenthanteringsprocess för att identifiera, spåra, logga, kategorisera och klassificera IKT-relaterade incidenter

Incidentrapportering*		
Initial anmälan	**Delrapport**	**Slutrapport**
• Initial rapport inom 4 timmar från klassificering av allvarlig incident	• Väsentligt ändrad status • Ändrad hantering • Efter återställning • Inom 72 timmar från att incident klassificerats som normal	• Efter 1 månad • Rotorskasanalys • Vidtagna åtgärder • Faktisk påverkan

Incidentklassificering*	
Kriterier för att bedöma allvarliga incidenter	
Antal påverkade kunder eller motparter	Ryktesmässig påverkan
Duration including service downtime	Geografisk påverkan
Förlust av data	Kritikaliteten i tjänsterna som påverkas
Finansiell påverkan	

* Utkast på tekniska standarder – kan komma att ändras

BG Institute
EN DEL AV BLENDOW GROUP

Tester på samtliga kritiska IT-system ska utföras minst årligen

IT-riskhantering | Incidenthantering | **Testning av IT-system** | Hantering av IT-leverantörsrisk

DORA kräver att finansiella entiteter upprättar, underhåller och löpande granskar ett sunt, riskbaserat och heltäckande digitalt testprogram för operativ motståndskraft

Några av kraven:

- Genomförande av tester på **alla kritiska IT-system och applikationer** minst årligen
- **För de största –** Avancerade tester baserat på hotbildsstyrda penetrationstester (**TLPT**) var tredje år enligt TIBER-EU-ramverket
- (Utkast teknisk standard) **Veckovis automatiserad sårbarhetsskanning**

BG Institute
EN DEL AV BLENDOW GROUP

Omfattande krav på IT-avtal, leverantörsprocess och dokumentation

IT-riskhantering | Incidenthantering | Testning av IT-system | **Hantering av IT-leverantörsrisk**

- Lämpliga kontraktuella relationer mellan IKT-leverantörer och finansiella entiteter stärker motståndskraften
- Tillsyn på EU-nivå över finansmarknadens kritiska IKT-leverantörer

Process för hantering av risker med IT-leverantörer
Operationella risker (såsom säkerhetsrisker, regulatoriska risker, datarisker) och prestanda ska bevakas genom hela livscykeln för ett IT-avtal

Inför avtal		Kontraktsfas		Upplösning
1 Urval och due diligence	2 Riskanalys	3 Avtalskrav	4 Löpande uppföljning	5 Exitplanering

BG Institute
EN DEL AV BLENDOW GROUP

Men vad gäller för IT-leverantörerna?

- **Kritiska IKT-tredjepartsleverantörer** kommer att **omfattas av tillsyn** av de s.k. ESA-myndigheterna på EU-nivå

- För varje utsedd kritisk IKT-leverantör kommer en **dedikerad plan för översyn** att tas fram och följas upp

- ESA-myndigheterna får **befogenheter att ingripa** mot de kritiska IKT-leverantörerna och även **tilldela straffavgifter**

- Kritiska IKT-leverantörer blir också **indirekt påverkade av DORA** eftersom finansiella entiteter behöver **uppdatera sina IT-avtal** och i vissa fall **inkludera leverantörerna i sina tester**

Andra cyberrelaterade EU-förordningar/direktiv

- NIS2-direktivet
- Critical Entities Resilience (CER)-direktivet
- Cyber Resilience Act (CRA)

Pass III
Några praktiska medskick och frågor

BG Institute
EN DEL AV BLENDOW GROUP

Några praktiska medskick för dig som arbetar med DORA i ett finansiellt bolag

- DORA är **inte bara ett IT-projekt –** kräver involvering från ledning, säkerhet, risk, juridik, ev. COO m.fl.

- Identifiera och **bygg förteckningen** över dina funktioner, IT- och informationstillgångar, IT-leverantörer – den kommer att vara centralt genom hela implementeringen

- Etablera tidigt i projektet dina **kritiska funktioner och IKT-tjänster** för att kunna fokusera på de väsentliga riskerna

- Om ni har **mycket utkontrakterad IT** – lägg vikt vid att identifiera och uppdatera era kritiska IT-avtal samt förstärk leverantörsprocessen

Fördjupningskurs den 3 september med Johan Lindfors:
Digital Operational Resilience Act (DORA)

Under kursdagen får du kunskap om:

- DORAs grundprinciper och regelkrav
- Hur man kan påbörja implementationsarbetet med DORA
- DORA i samklang med AI och integritetsskydd

Boka din plats via länken!

BG Institute
EN DEL AV BLENDOW GROUP

Vad tyckte du om dagens webbinarium?

Ta gärna 30 sekunder och svara på frågorna i fliken “Polls” under chattfliken.

Tack för dina synpunkter!

BG Institute
EN DEL AV BLENDOW GROUP

Frågor?

Johan Lindfors
PwC Sverige
t: +46 (0) 70 393 4899
m: johan.lindfors@pwc.com

BG Institute
EN DEL AV BLENDOW GROUP