Policy

BESLUTSDATUM:	2018-05-22
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	STA/RIE
FÖRVALTNINGSANSVARIG:	Lars Andersson

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

Senast granskad: 2018-05-22

DNR [Diarienummer]

Informationssäkerhet

Denna policy anger Riksbankens inriktning och övergripande principer för informationssäkerhet, liksom roller och definitioner inom området.

Information är en viktig tillgång för Riksbanken. Rätt information med rätt kvalitet, i rätt tid, på rätt plats till rätt personer är en förutsättning för att Riksbanken ska kunna utföra sitt uppdrag och nå sina mål.[1]

Information som kommer obehöriga till del, är felaktig eller manipulerad eller som inte är tillgänglig när den behövs, kan orsaka stora skador på Riksbankens verksamhet, innebära kostnader och påverka samhällets förtroende för Riksbanken. Information måste därför skyddas i enlighet med denna policy.

Informationssäkerhet är en del av arbetet med operativa risker. Informationssäkerhet innefattar också både IT-säkerhet och Cybersäkerhet. En något förenklad organisatorisk gränsdragning mellan informations- och IT-säkerhet är att informationssäkerhetsarbetet beskriver VAD som ska göras (inklusive IT-säkerhet) medan IT-säkerhetsarbetet beskriver HUR det ska göras.

Informationssäkerhet är också en väsentlig del i upprätthållandet av Riksbankens säkerhetsskydd som syftar till att skydda den verksamhet som är av vikt för rikets säkerhet.[2]

Definitioner

Informationssäkerhet - bevarande av konfidentialitet, riktighet och tillgänglighet hos information, oberoende av form; talad, tryckt, elektronisk etc.

IT-säkerhet - åtgärder för att upprätthålla informationssäkerhet i IT-system.

[1] Policy för Riksbankens informationsförsörjning (2018-00441).
[2] Säkerhetspolicy (2015-144-STA).

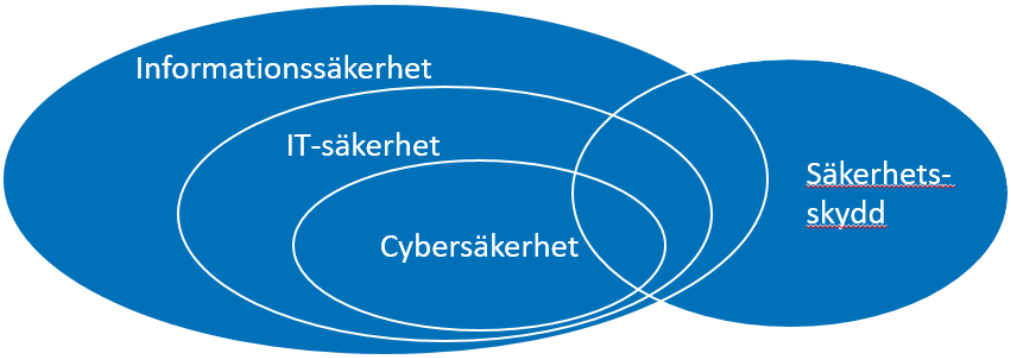
Cybersäkerhet – Tekniska och administrativa åtgärder till skydd mot fientliga eller illvilliga, externa IT-hot.

Säkerhetsskydd – skydd mot spionerи, sabotage och andra brott som kan innebära hot mot rikets säkerhet, innefattande informationssäkerhet, tillträdeskontroll samt säkerhetsprövning.

Konfidentialitet - egenskapen att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Riktighet - egenskapen att information är korrekt och fullständig.

Tillgänglighet - egenskapen att information är åtkomlig och användbar på begäran från ett behörigt objekt.



Principer

- Arbetet med informationssäkerhet ska följa gällande lag och rätt.
- Arbetet med informationssäkerhet ska bedrivas i enlighet med ett ledningssystem för informationssäkerhet, LIS.[3]
- Information ska klassificeras med avseende på konfidentialitet.
- IT-system och IT-tjänster ska, med utgångspunkt från informationens värde, klassificeras med avseende på konfidentialitet, riktighet och tillgänglighet.
- Varje viktig informationsmängd bör ha en utsedd ägare.
- Varje IT-system och IT-tjänst ska ha en utsedd ägare.
- Information och IT-system ska skyddas i enlighet med klassificeringen.
- Det ska finnas regler och andra styrande dokument som stöd i informationssäkerhetsarbetet.
- Kostnaden för skyddsåtgärder ska vägas mot värdet av det som skyddas.
- Informationssäkerheten ska ta hänsyn till verksamhetens krav på funktion.
- Informationssäkerhet ska beaktas under informationens och IT-systemens hela livscykel, från upprättande/införande till avveckling/destruktion.

[3] Ett Ledningssystem för Informationssäkerhet (LIS) syftar till att utveckla, införa och förvalta ett ramverk för att hantera säkerheten för organisationens informationstillgångar. Standarden ISO/IEC 27000 är vad som vanligen avses med ett LIS men det finns andra ramverk som också kan användas.

- Alla medarbetare och all inhyrd personal ska ha tillräckliga kunskaper i informationssäkerhet i relation till sina arbetsuppgifter så att den avsedda säkerhetsnivån kan upprätthållas.
- Incidenter ska rapporteras och följas upp.
- Informationssäkerhetens effektivitet ska kontinuerligt följas upp och vid behov justeras.
- Verksamhetens behov av kontinuitet i IT-miljön ska tillgodoses.
- Väsentliga händelser i Riksbankens IT-miljö ska loggas och sparas under den tid som behövs för att kunna utreda oegentligheter och incidenter.
- ECBS regelverk för informations[4]- och IT-säkerhet[5] ska tillämpas där ECBS-information lagras, bearbetas och överförs.
- Riksbanken ska, i sin roll som FMI (Financial Market Infrastructure) tillämpa de regelverk och rekommendationer inom informationssäkerhet som gäller branschen i övrigt.[6]

Roller och ansvar

Direktionen fastställer denna policy samt beslutar om inriktning och tilldelar resurser via budget och verksamhetsplan. Direktionen informeras löpande om informationssäkerhetsläget och tar vid behov beslut om informationssäkerhetsfrågor som överlämnats från informationssäkerhetschefen.

Informationssäkerhetschefen ansvarar för det övergripande arbetet med informationssäkerhetsfrågor vilket innebär stöd och uppföljning inom området, att utveckla modeller och metoder för hantering av informations-, IT- och cyberrisker, att lämna förslag till regler samt att rapportera informationssäkerhetsläget till direktionen och andra intressenter. Informationssäkerhetschefen ansvarar också för den övergripande utbildningen i informationssäkerhet till medarbetare och andra användare av Riksbankens information. Informationssäkerhetschefen ingår i den andra försvarslinjen[7]

Avdelningschef ansvarar för att samtliga risker, inklusive informationssäkerhetsrisker, hanteras inom sitt verksamhetsområde.

Medarbetare ansvarar för att följa regler och rutiner inom området samt rapportera incidenter och händelser som kan innebära hot mot informationssäkerheten.

Riskchefen ansvarar för en oberoende uppföljning och rapportering av Riksbankens operativa risker.

Säkerhetschefen, tillika **säkerhetsskyddschef**, ansvarar för Riksbankens säkerhetsskydd vilket även innefattar informationssäkerhet för de delar av Riksbankens verksamhet som är av vikt för rikets säkerhet. Säkerhetschefen samråder i dessa frågor med informationssäkerhetschefen.

[4] Common rules and minimum standards for the handling of sensitive ESCB information).
[5] ESCB information systems security policy (SEC/GovC/X/16/1623a - SEC/GenC/X/16/092a).
[6] Exempelvis CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.
[7] Policy för intern styrning och kontroll (2016-00498).

IT-chefen ansvarar för att Riksbankens IT-miljö uppfyller verksamhetens behov av informations- och IT-säkerhet, oavsett om den bedrivs i egen regi eller är utkontrakterad.

IT-säkerhetsansvarig ansvarar för att IT-säkerhetsåtgärder införs och förvaltas så att de uppfyller Riksbankens övergripande informationssäkerhetskrav samt att tillhandahålla dokumentation och andra hjälpmedel för användning av IT-säkerhetsfunktioner.

Informationsägare ansvarar för att klassificera information inom sitt verksamhetsområde och ska säkerställa att den hanteras i enlighet med Riksbankens regler inom området. Informationsägaren ansvarar också för att hantera och om så krävs acceptera risker kring informationen överallt där den hanteras, lagras och transporteras.

Objektägare (systemägare) ansvarar för att informationssäkerheten hålls på avsedd nivå i sina IT-system på uppdrag av informationsägarna.