RISKANALYS OCH SÄKERHETSSTYRNING
Stockholms Läkarhus AB
Tillämpning av NIST RMF i en fiktiv, medelstor, privat aktör i Stockholms läns primärvård.

INTRODUKTION

Om NIST Risk Management Framework:
NIST Risk Management Framework (RMF) är en strukturerad metodik för att integrera säkerhet och integritetsskydd i systemutvecklingens livscykel. RMF utvecklades av U.S. National Institute of Standards and Technology och används globalt som de facto-standard för riskbaserad säkerhetsstyrning.

Fördelar med RMF:
- Strukturerad process: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor som säkerställer att ingen del av säkerhetsarbetet förbises
- Riskbaserad approach: Säkerhetsåtgärder anpassas efter faktisk risk snarare än "check-box compliance"
- Livscykelperspektiv: Kontinuerlig monitorering istället för punktinsatser
- Internationellt erkänt: Underlättar kommunikation med partners, leverantörer och revisorer

Begränsningar för svensk kontext:
RMF är utvecklat för amerikanska federala myndigheter och använder därför amerikanska standarder. För svensk tillämpning krävs anpassning till svenska lagar (Cybersäkerhetslagen, GDPR, Patientdatalagen), MCF:s metodstöd för informationssäkerhet, samt svenska myndigheters terminologi (IMY, MCF, IVO). Detta dokument tillämpar RMF:s struktur men använder svenska lagar och MCF-metodik för klassning och riskvärdering.

Organisation:
Stockholm Läkarhus AB är en privat vårdgivare som bedriver primärvård genom sex vårdcentraler i Stockholms län. Verksamheten omfattar:
- 40 läkare, 55 sjuksköterskor, 30 administrativ personal
- Ca 60 000 listade patienter på 6 vårdcentraler
- Årlig omsättning: 75 miljoner SEK
- IT-miljö: Journalsystem för patientjournalföring, tidsbokning via webb och app, e-recept via Nationellt Läkemedelsregister, journaldelning via Nationell Patientöversikt

Juridisk omfattning:
- Cybersäkerhetslagen: Viktig enhet som kräver riskanalys (2 kap. 3§), incidentrapportering till CSIRT som ingår i MCF enligt Cybersäkerhetsförordningen.
- GDPR Art. 9: Känsliga personuppgifter som hälsodata kräver tekniska säkerhetsåtgärder enligt Art. 32 och rapportering till IMY enligt Art. 33
- Patientdatalagen 2 kap. 2§: Patientsäkerhet och skydd mot obehörig åtkomst

1. RMF PREPARE: RISK MANAGEMENT STRATEGY

Syfte med Prepare-steget:
Prepare-steget etablerar organisatoriska förutsättningar och riskhanteringsstrategi som krävs för att framgångsrikt genomföra de efterföljande RMF-stegen.

Riskacceptans:
Nolltolerans mot risker som kan leda till patientskador, GDPR-böter eller betydande incidenter som orsakar 'allvarlig driftsstörning' enligt Cybersäkerhetslagen 2 kap. 5§.

Roller och ansvar:
Stockholm Läkarhus AB (vårdgivare) är personuppgiftsansvarig enligt Patientdatalagen 2 kap. 6§ och GDPR Art. 4(7). Ledningen verkställer företagets skyldigheter enligt följande rollfördelning:

- VD: Yttersta ansvar, godkänner policy, riskacceptans och systemauktorisering. Delegerar operativt genomförande.
- IT-chef: Systemägare, implementerar tekniska kontroller, daglig drift.
- DPO/CISO: Leder informationssäkerhetsarbete och GDPR-compliance, rapporterar incidenter till IMY (GDPR Art. 33) och MCF (Cybersäkerhetsförordningen 6§).
- Verksamhetschefer: Verkställer informationssäkerhet vid respektive vårdcentral.

Systemgräns:
Journalsystemet omfattar patientjournalföring för alla sex vårdcentraler. Systemet inkluderar applikationsserver, databas, autentisering, loggning och backup (lokal NAS). Exkluderas: NPÖ, e-recept (externa via E-hälsomyndigheten), tidsbokningssystem, nätverksinfrastruktur (common controls).

Informationstyper:
- Patientjournaler: Namn, personnr, diagnos, behandling, mediciner, anteckningar
- Personaluppgifter: Namn, personnr, legitimation, behörigheter
- Åtkomstloggar: Användar-ID, tidsstämpel, åtkomst till journal

Metodik och frekvens:
K-R-T (Konfidentialitet-Riktighet-Tillgänglighet) med konsekvensnivåer enligt MCF-metodstöd: Allvarlig (högsta), Betydande, Måttlig, Försumbar (lägsta). Riskbedömning: RISK = SANNOLIKHET × KONSEKVENS.

Stockholm Läkarhus AB använder fem konsekvensnivåer för riskanalys och informationsklassning anpassat efter MCF-metodstöd för informationssäkerhet:

Nivå	Beteckning	Beskrivning
4	Synnerligen allvarlig	Betydelse för Sveriges säkerhet (Säkerhetsskyddslagen)
3	Allvarlig	Kan leda till dödsfall, livshotande situation, kritisk verksamhetspåverkan, eller mycket stora ekonomiska konsekvenser
2	Betydande	Allvarlig skada (ej livshotande), betydande verksamhetspåverkan, eller stora ekonomiska konsekvenser
1	Måttlig	Märkbar skada eller påverkan, måttliga ekonomiska konsekvenser
0	Försumbar	Minimal eller ingen påverkan, försumbara ekonomiska konsekvenser

Årlig riskanalys enligt Cybersäkerhetslagen 2 kap. 3§, kvartalsvis ledningsgenomgång enligt branschpraxis, kontinuerlig loggmonitorering enligt Patientdatalagen 4 kap. 3§.

2. RMF CATEGORIZE: SYSTEMKATEGORISERING

Syfte med Categorize-steget:
Categorize-steget klassificerar information och system baserat på potentiell konsekvens vid förlust av konfidentialitet, riktighet eller tillgänglighet.

Informationsklassning:

Informationstyp	K-R-T
Patientjournaler	K3-R3-T3
Personaluppgifter	K1-R1-T0
Åtkomstloggar	K2-R3-T1

Klassning av patientjournaler (K3-R3-T3):

- Konfidentialitet = K3 (Allvarlig)
    - Juridisk grund: GDPR Art. 9 känsliga personuppgifter, Patientdatalagen 2 kap. 2§
    - Konsekvens: GDPR-böter upp till 4% av omsättning (3 MSEK), exponerade skyddade identiteter kan innebära livsfara
    - Klassning: K3 (Allvarlig) - Näst högsta skyddsnivå krävs för känsliga personuppgifter med potentiellt livshotande konsekvenser

- Riktighet = R3 (Allvarlig)
    - Juridisk grund: Patientdatalagen 3 kap. 2§ (journalens syfte), Patientsäkerhetslagen 6 kap. 1§ (arbete enligt vetenskap och beprövad erfarenhet)
    - Konsekvens: Felaktig medicininformation kan leda till patientskada eller dödsfall
    - Klassning: R3 (Allvarlig) - Högsta skyddsnivå krävs då felaktig information kan leda till dödsfall

- Tillgänglighet = T3 (Allvarlig)
    - Juridisk grund: Cybersäkerhetslagen 2 kap. 5§, Patientdatalagen 3 kap. 2§
    - Konsekvens: Primärvården stannar helt dvs driftstopp kräver MCF-rapportering inom 24 timmar.
    - Klassning: T3 (Allvarlig) - Näst högsta skyddsnivå krävs då kärnverksamheten är helt beroende av systemet

Systemkategorisering:
Journalsystemets klassning: K3-R3-T3. Aggregeringseffekt: 60 000 patientjournaler innebär att systemkompromiss påverkar samtliga patienter samtidigt, vilket förstärker konsekvenserna. Klassningen styr valet av säkerhetsåtgärder i nästa steg.

3. RMF SELECT: VAL AV SÄKERHETSÅTGÄRDER

Syfte med Select-steget:
Select-steget väljer säkerhetsåtgärder baserat på systemets K3-R3-T3 klassning och juridiska krav från Cybersäkerhetslagen, GDPR och Patientdatalagen.

Juridisk grund:
Cybersäkerhetslagen 2 kap. 3§ kräver säkerhetsåtgärder för riskanalys och systemsäkerhet (punkt 1), incidenthantering (punkt 2), kontinuitetshantering (punkt 3), samt strategier för åtkomstkontroll (punkt 9) och kryptografi (punkt 8).
GDPR Art. 32(1) kräver kryptering (a), konfidentialitet och integritet (b), återställning vid incident (c), regelbunden testning (d).
Patientdatalagen 4 kap. kräver begränsad behörighet (2§), åtkomstdokumentation och systematiska kontroller (3§), patientspärr (4§).

Valda säkerhetsåtgärder:

ÅTKOMSTKONTROLL:
- Multifaktorsautentisering (MFA) med lösenord + BankID
- Rollbaserad åtkomstkontroll (RBAC): Läkare (läs/skriv på sin vårdcentral), sjuksköterska (begränsat till omvårdnad), administrativ personal (endast schemaläggning)
- Patientspärr enligt Patientdatalagen 4 kap. 4§

KRYPTERING:
- Databaskryptering: AES-256 (branschstandard), nycklar i Hardware Security Module
- TLS 1.3 för all kommunikation mellan klient och server

LOGGNING OCH MONITORERING:
- Detaljerad åtkomstloggning (varje journalöppning loggas)
- Månatliga loggkontroller av IT-chef (Patientdatalagen 4 kap. 3§)
- Automatiska larm vid >5 misslyckade inloggningar eller >50 journalöppningar/timma

INCIDENTHANTERING:
- Parallella rapporteringsprocesser: Säkerhetsincident till MCF enligt Cybersäkerhetsförordningen (upplysning inom 24 timmar (Cybersäkerhetslagen 2 kap. 5§), incidentanmälan inom 72 timmar (2 kap. 6§), slutrapport inom 1 månad (2 kap. 8§)), personuppgiftsincident till IMY (inom 72 timmar enligt GDPR Art. 33)
- Årlig ransomware-övning

KONTINUITETSHANTERING:
- Daglig inkrementell backup + veckovis full backup till offsite enligt branschpraxis
- Återställning testas kvartalsvis, mål: systemet operativt inom 4-8 timmar
- Dokumenterade instruktioner vid nödfall på papper vid driftstopp

Common controls enligt NIST RMF (IT-avdelningen): Brandväggar, IDS, fysisk serversäkerhet, sårbarhetshantering.

4. RMF IMPLEMENT: IMPLEMENTATION

Syfte med Implement-steget:
Implement-steget genomför de valda säkerhetsåtgärderna genom policy, teknisk konfiguration och organisatoriska processer.

Säkerhetspolicy:
Informationssäkerhetspolicy (godkänd VD 2026-01-01) fastställer krav på MFA, förbud mot delning av inloggningsuppgifter, rapportering internt av incidenter inom 1 timme.

Teknisk implementation:

- Genomfört 2025: Databaskryptering (AES-256), TLS 1.3, daglig + veckovis backup, RBAC, åtkomstloggning
- Kommande 2026: MFA-lösning (BankID), automatiska larm, kvartalsvis backup-testning

Organisatoriska åtgärder:

- Säkerhetsutbildning för all personal (omgående): Phishing awareness, lösenordshygien, incidentrapportering
- Månatliga loggkontroller av IT-chef (pågående)
- Kvartalsvis behörighetsgranskning (omgående)
- Årlig incidentövning (i år)

5. RMF ASSESS: RISKANALYS

Syfte med Assess-steget:
Assess-steget identifierar och värderar specifika hot och sårbarheter mot journalsystemet för att prioritera åtgärder.

Hotbild:

Hot	Sannolikhet	Konsekvens	Risk	Åtgärd
Ransomware	HÖG	ALLVARLIG (K3-R3-T3)	KRITISK	MFA (omgående), awareness-utbildning (omgående), backup-testning (omgående)
Insiderhot	MEDEL	BETYDANDE (K2)	HÖG	Automatiska larm (i år), månatliga loggkontroller (pågående)
Phishing	HÖG	ALLVARLIG (K3-R3-T3)	KRITISK	MFA (omgående), phishing-simulering (i år)
Hårdvarufel	MEDEL	ALLVARLIG (T3)	HÖG	Kvartalsvis backup-test (omgående), redundant server (i år)
DDoS	LÅG	BETYDANDE (T2)	MEDEL	Monitorera, ingen omedelbar åtgärd behövs

Sårbarheter:

- Tekniska: MFA ej implementerad ännu, backup-testning endast årlig
- Organisatoriska: Begränsad säkerhetsutbildning, ingen genomförd incidentövning

Restrisker:
Även efter implementering kvarstår risk för ransomware (zero-day sårbarheter) och insiderhot (personal med legitim åtkomst). Dessa restrisker accepteras av VD efter implementering av MFA, loggning och larm.

6. RMF AUTHORIZE: RISKACCEPTANS

Syfte med Authorize-steget:
VD granskar riskanalysen, implementerade kontroller och restrisker för att fatta formellt beslut om systemet får användas.

VD:s bedömning:
Journalsystemet är kritiskt för vårdverksamheten (K3-R3-T3). Genomförda säkerhetsåtgärder (kryptering, backup, loggning, RBAC) uppfyller grundläggande krav enligt Cybersäkerhetslagen, GDPR och Patientdatalagen. Restrisker (ransomware, insiderhot) bedöms acceptabla efter implementering av MFA, larm, utbildning.

Beslut:
VD AUKTORISERAR journalsystemet för fortsatt drift med villkor:

- MFA implementerad senast 2026-03-01
- Automatiska larm implementerade senast 2026-04-01
- Säkerhetsutbildning genomförd senast 2026-05-01

Auktoriseringsperiod: 2026-01-15 till 2027-01-15 (12 månader).

7. RMF MONITOR: KONTINUERLIG MONITORERING

Syfte med Monitor-steget:
Monitor-steget säkerställer kontinuerlig övervakning av säkerhetsåtgärder, hot och sårbarheter.

Teknisk monitorering:

- Daglig backup-status (automatisk rapport till IT-chef)
- Månatlig genomgång av åtkomstloggar
- Kvartalsvis sårbarhetsskanning och backup-test

Organisatorisk monitorering:

- Kvartalsvis ledningsgenomgång (VD, IT-chef, DPO & CISO)
- Kvartalsvis behörighetsgranskning
- Årlig incidentövning och riskanalys

Incidentrapportering:
Vid säkerhetsincident: CISO anmäler till MCF (CSIRT-enheten) enligt Cybersäkerhetsförordningen 6§ (**upplysning** inom 24 timmar (Cybersäkerhetslagen 2 kap. 5§), **incidentanmälan** inom 72 timmar (2 kap. 6§), **slutrapport** inom 1 månad (2 kap. 8§)).
Vid personuppgiftsincident: DPO anmäler till IMY (inom 72 timmar enligt GDPR Art. 33).
Kvartalsrapport till VD: Antal incidenter, implementationsstatus, loggkontroller, sårbarheter.

Uppdatering av riskanalys:
Triggers för omedelbar riskbedömning: Ny kritisk sårbarhet (CVSS >9.0), ransomware-attack mot svensk vård, lagändring, allvarlig incident.
Årlig fullständig riskanalys för förnyat auktoriseringsbeslut inför kommande kalenderår.