Instruktion

Beskrivning av flikar

Sammanfattning: Här presenteras sammanfattning av genomförda riskbedömningar sa

Hot: Här finns stöd för identifiering av hot som kan användas vid behov.

Sårbarheter: Här finns stöd för identifiering av sårbarheter som kan användas vid beho

Riskbedömning: Här ska risker dokumenteras och bedömas.

Riskbehandling: Här ska risker som inte accepteras och som kräver behandling väljas ge
kolumn A och dokumentera information om vilka ytterligare åtgärder som krävs.

Tillvägagångssätt

Riskbedömningen startar i fliken "Riskbedömning" där man går höger till vänster. Kolur
sårberheter och hot för att underlätta att skriva rätt typ av riskscenarier. Det är alltså in
direkt kan komma på och sammanställa rätt typ av riskscenarier som krävs för analysob
en sammansättning av hot - sårbarheter - konsekvens kan med fördel raderna emellan
riskbehandling kan acceptanskriterierna som återfinns i fliken "Sammanfattning" använ

Alla risker som inte accepteras bör också tas med i fliken "Riskbehandling". Väl rätt typ
kolumn A. Kolumn B-D fylls då i automatiskt och kolumnerna E-H fylls i själva av deltaga

Uppdatering av mall

Behöver olika alternativ uppdateras, uppdatera informationen i fliken "Data". Denna fli
högerklicka på någon flik och välj "Ta fram" och välj sedan "Data".

Här kan namn på olika saker, eller listor uppdateras då andra flikar hämtar information

Notera: Om antalet alternativ i listor eller liknande ökas kan eventuellt området för list
välja "Data" i menyfliken (dvs inte excelfliken data), välja dataverifiering och välja rätt c

amt acceptanskriterier.

v.

enom att välja rätt risk ID i drop down i

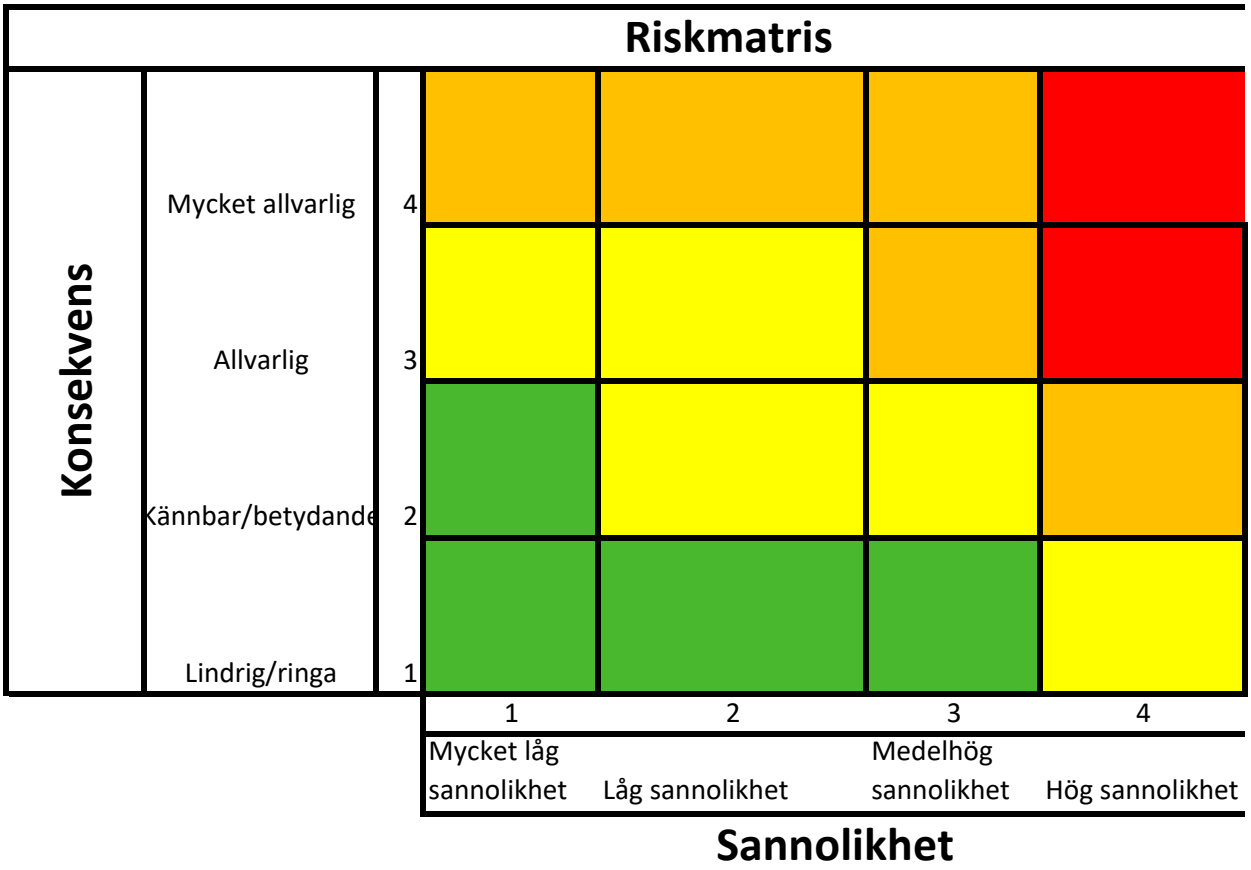
nnerna A-D kan användas för att samla olika
nte obligatoriskt om man känner att man
bjektet. Om fler riskscenarier skapas utifrån
kolumn A-D sammanfogas. Vid val av
ndas för att säkerställa att dessa efterlevs.

av risker genom att använda drop down i
arna.

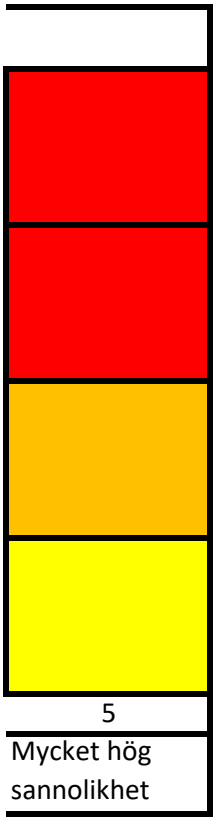
iken är generellt dold, för att ta fram

en från denna flik.

orna också utökas. Göra detta genom att
område där listan ska hämtas ifrån


Riskmatris
Konsekvens
Mycket allvarlig
4
Allvarlig
3
Kännbar/betydande
2
Lindrig/ringa
1
1
2
3
4
Mycket låg sannolikhet
Låg sannolikhet
Medelhög sannolikhet
Hög sannolikhet
Sannolikhet

Sammanfattning ris



Antal risker		%
Oacceptabel nivå	0	#DIVISION/0!
Hög nivå	0	#DIVISION/0!
Medelhög nivå	0	#DIVISION/0!
Acceptabel nivå	0	#DIVISION/0!

Risknivå
Oacceptabel nivå
Hög nivå
Medelhög nivå
Acceptabel nivå

Skala för riskacceptans

Bedömning	Risk får accepteras av
Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats med hög sannolikhet eller hög konsekvens. Riskerna kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning
Höga risker som behöver åtgärdas. Riskerna kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning
Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.	Riskägare
Risker som inte kräver någon åtgärd alternativt bedömts som låga och/eller bedömts inte medföra störningar i organisationen. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den löpande verksamheten.	Riskägare

Krav på information	Krav på behandling	Riskregister
Ledning, styrelse och bolags-controller	Snarast	Övergripande och lokalt
Ledning	Inom 3 månader	Övergripande och lokalt
Ansvarig chef	Inom 12 månader	Övergripande och lokalt
Inga krav	Inga krav	Lokalt

Exempel hot

Hottyp	Hot	Exempel
Cyberhot	Ransomware	
	Malware	Virus, trojan, worms
	Social engineering	Phishing, piggy backing, dumpster diving
	Dataintrång (intentional)	
	Dataläcka (unintentional)	
	Data manipulation	
	DDOS	
	Nätverksattacker	Spoofing, MITM
Tillgänglighetsförlust	Systemfel	
	Funktionsförlust	
	Kapacitetsproblem	
	Driftstörning	Strömavbrott, kommunikationsavbrott (internet, telefoni) etc etc
Samhällshot	Naturliga och fysiska	Snöstorm, värmebölja, brand, översvämning
	Yttre påverkan	Immigration, strejk, inflation
	Konflikt	Sabotage, terrorism, vandalism, krig
Informationsförlust	Systemfel	
	Felaktig radering av information	
	Dataintrång	
	Felaktig förändring av information	
Oegentligheter	Bedrägeri	Identitetskapning, Falska upphandlingar eller avtal
	Stöld	
	Jäv	
	Bestickning	
GRC	Otillräcklig insyn/övervakning	
	Bristande efterlevnad av lagkrav	Dataskyddsbrott, DORA
	Bristande efterlevnad interna regler	Code of conduct, styrning
Tredjepart/utkontraktering	Leverantörsberoende	Inlåsningseffekt
	Brister i avtal	
	Incidenter hos leverantör	

Exempel sårbarheter

Kategori	Sårbarhet
Hårdvara	Otillräckligt fysiskt skydd av hårdvara
	Otillräckligt underhåll
	felaktig installation
	Otillräcklig konfigurering av hårdvara (Ex. BIOS, firmware, embedded)
	Oskyddad lagring (ex. okrypterad hårdvara)
Programvara	Ouppdaterad programvara (bristande patchrutiner)
	Sårbara eller otillräckliga standardkonfigurationer
	Felaktiga konfigurationer (dvs som inte följer org. Satta standard)
	Bristande inputvalidering
	Sårbara API:er
	Otillräcklig testning
	Sårbara integrationer mellan system och tjänster
	Otillräcklig eller bristande dokumentation
	Otillräcklig eller bristande kryptering (ex. för svaga protokoll, otillräckligt skydd av kryptografiska nycklar)
	Komplicerat användargränssnitt
	Otillräcklig loggning
	Onödiga eller osäkra tjänster som har aktiverats
	Okontrollerad nedladdning och användning av programvara
	Bristande eller ofullständiga säkerhetskopior
Identitet och åtkomst	Svaga autentiseringsmekanismer (ex. svaga lösenord utan mfa)
	Delade konton
	Bristande sessionshantering
	Felaktig behörighetstilldelning (t.ex. för många har för höga behörigheter)
	Bristande eller otillräcklig granskning av behörigheter
	Behörigheter som inte uppdateras vid byte av roll

	Bristfällig hantering av avslutade konton
Personal	Bristande säkerhetsmedvetenhet
	Mänsklig faktor
	Bristande kontroll vid anställning
	Ingen återkommande utbildning
Organisation	Otillräcklig eller otydlig styrning
	Otillräcklig identifiering eller dokumentation av lagkrav eller risk
	Otydlig ansvarsfördelning
	Komplexa eller ineffektiva processer
	Låg prioritering av säkerhetsfrågor
	Otillräcklig eller otydlig kommunikation av interna rutiner
	Otillräckliga eller bristande granskningar/revisioner
	Analyser/bedömningar som inte görs systematiskt
	Otillräckliga resurser
Nätverk	Otillräcklig segmentering
	Osäkra eller oskyddade nätverk
	Otillräcklig kryptering
	Användning av sårbara IoT-enheter
Fysiska	Otillräckligt skalskydd
	Obevakade arbetsstationer
	Brist på loggar över in- och utpassering
	Åtkomst som inte avslutas efter avslutad anställning
	Obevakade eller okontrollerade leveranser
Leverantör och tredjepart	Otillräcklig kravställning
	Otillräckliga avtal (ex. SLA, NDA, PuB-avtal)
	Otillräcklig kontroll av leverantörs säkerhetsåtgärder
	Sårbarheter hos leverantör

Riskbedömning

Riskområde ID	Hot

Exempel på relevanta sårbarheter	Konsekvenser	Riskscenario ID

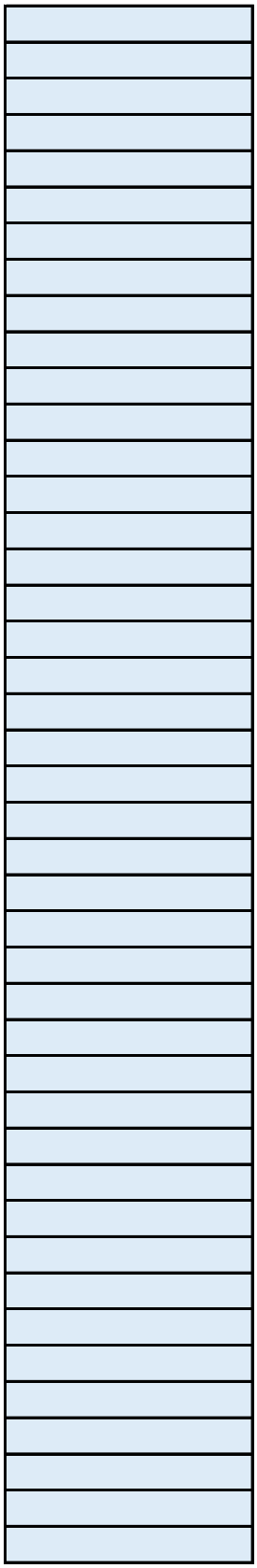
Riskbeskrivning "på grund av (sårbarhet) händer (hot) vilket leder till (konsekvens)"	Sannolikhet utan åtgärd

Konsekvens utan åtgärd	Riskvärde utan åtgärd	Sannolikhet med åtgärd	Konsekvens med åtgärd	Riskvärde med åtgärd

Kategori	Underkategori	Tema/mål	Process

Kommentar (/förtydligande/beskrivning av bedömt scenario)	Riskägare

Riskbehandling



Riskbehandling

Riskscenario ID	Riskbeskrivning	Riskvärde	Riskbehandling

Åtgärdsförslag	Åtgärdsansvarig

Tidplan	Status

Riskbehandling

Riskscenario ID	Riskbeskrivning

Riskvärde	Riskbehandling	Åtgärdsförslag

Åtgärdsansvarig	**Tidplan**	**Status**