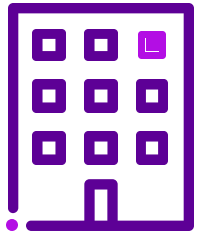


NIS2

FASTIGHETSBRANSCHEN

itm8

Shadi Domat

VERKSAMHETSKONSULT GRC

shadi.domat@itm8.com

itm8

AGENDA

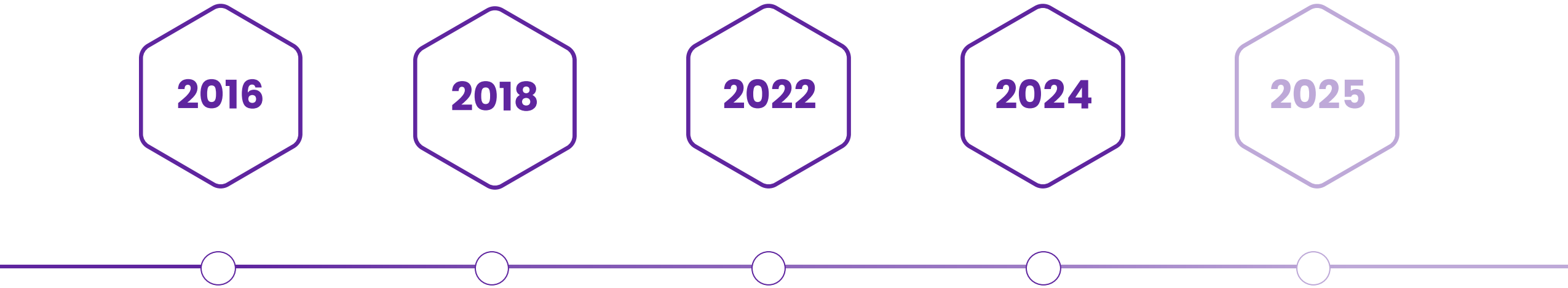
- Kort om NIS2
- Gemensam basplatta
- Vilka som omfattas
- Varför ni är här
- Funderingar och farhågor
- Vad ni behöver göra

itm8

NIS2 I SNABBA DRAG

NIS-RESAN

OCH HUR DEN HAR UTVECKLATS



NIS

Europaparlamentet och rådet antar direktivet för en hög gemensam nivå på säkerhet i nätverks- och informations-system

SVENSK LAG

NIS blir en svensk lag (2018:1174)

NIS 2

NIS upplevdes tandlöst. NIS2 antogs 14 dec 2022 och omfattar fler sektorer, hårdare krav och man inför tuffare påföljder.

TILLÄMPANDE

NIS2-direktivet börjar tillämpas i alla medlemsstater den 18 okt 2024

SVENSK LAG

”Cybersäkerhetslagen” föreslås börja tillämpas senare under 2025.

itm8

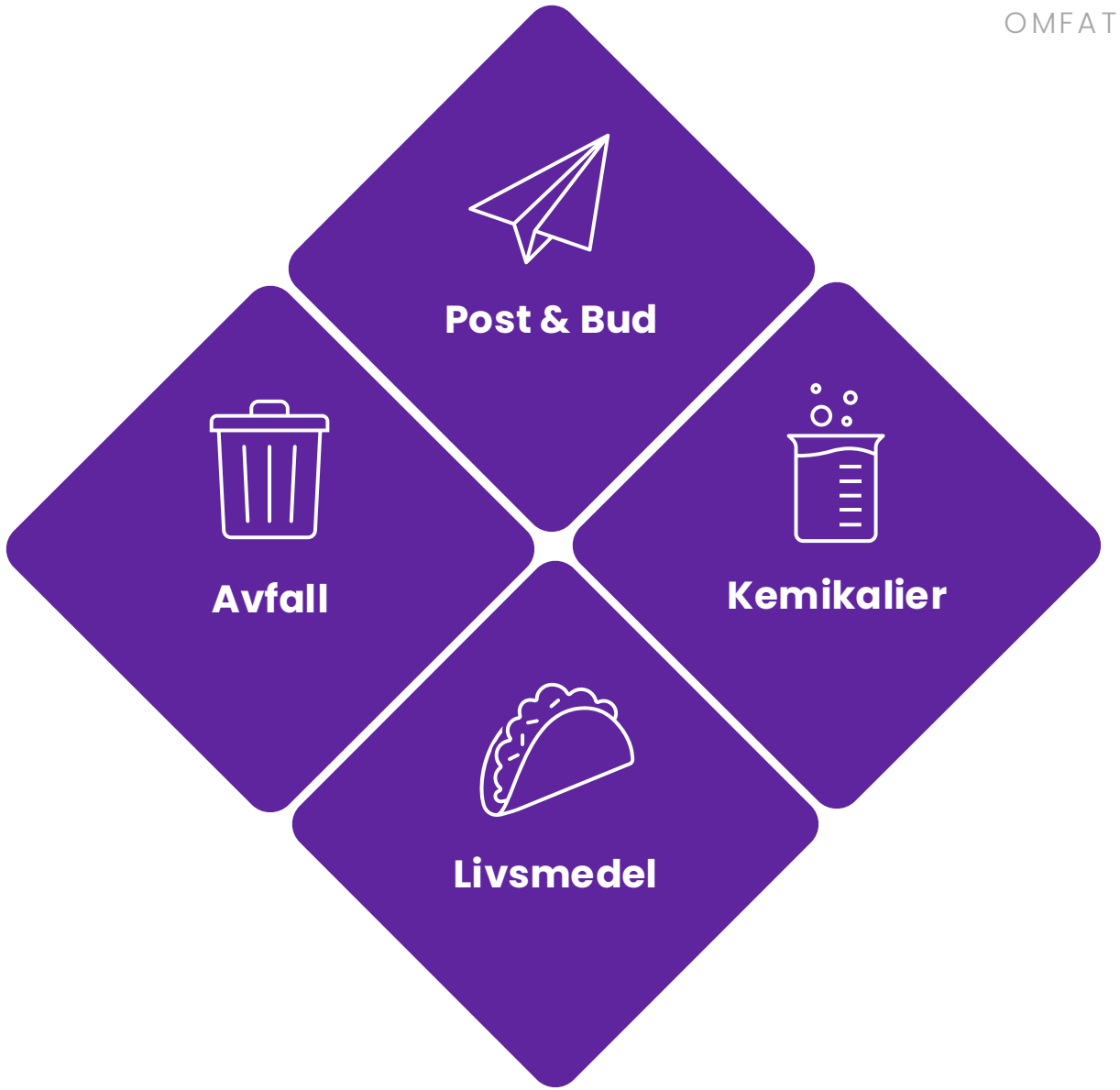
VILKA OMFATTAS?

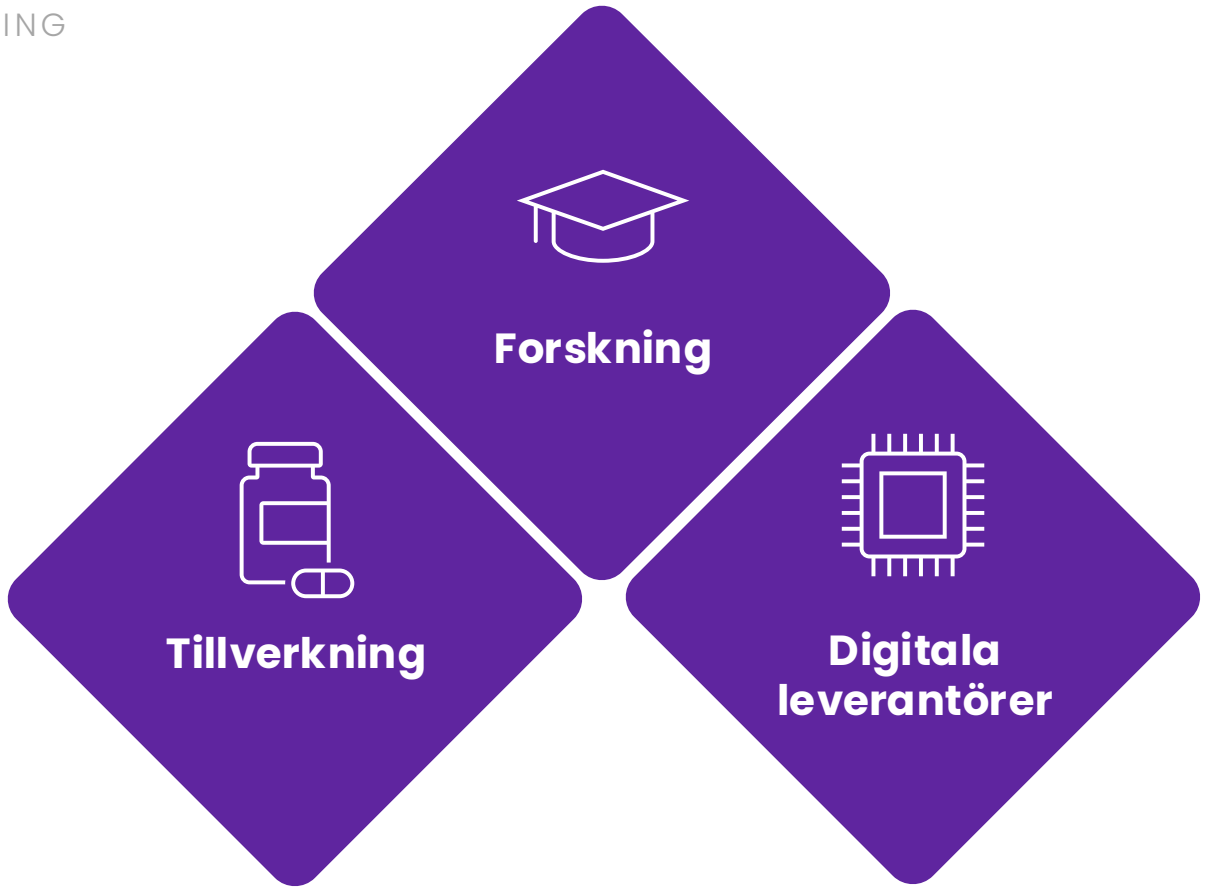
VIKTIGA ENTITETER

VÄSENTLIGA ENTITETER

VIKTIGA ENTITETER

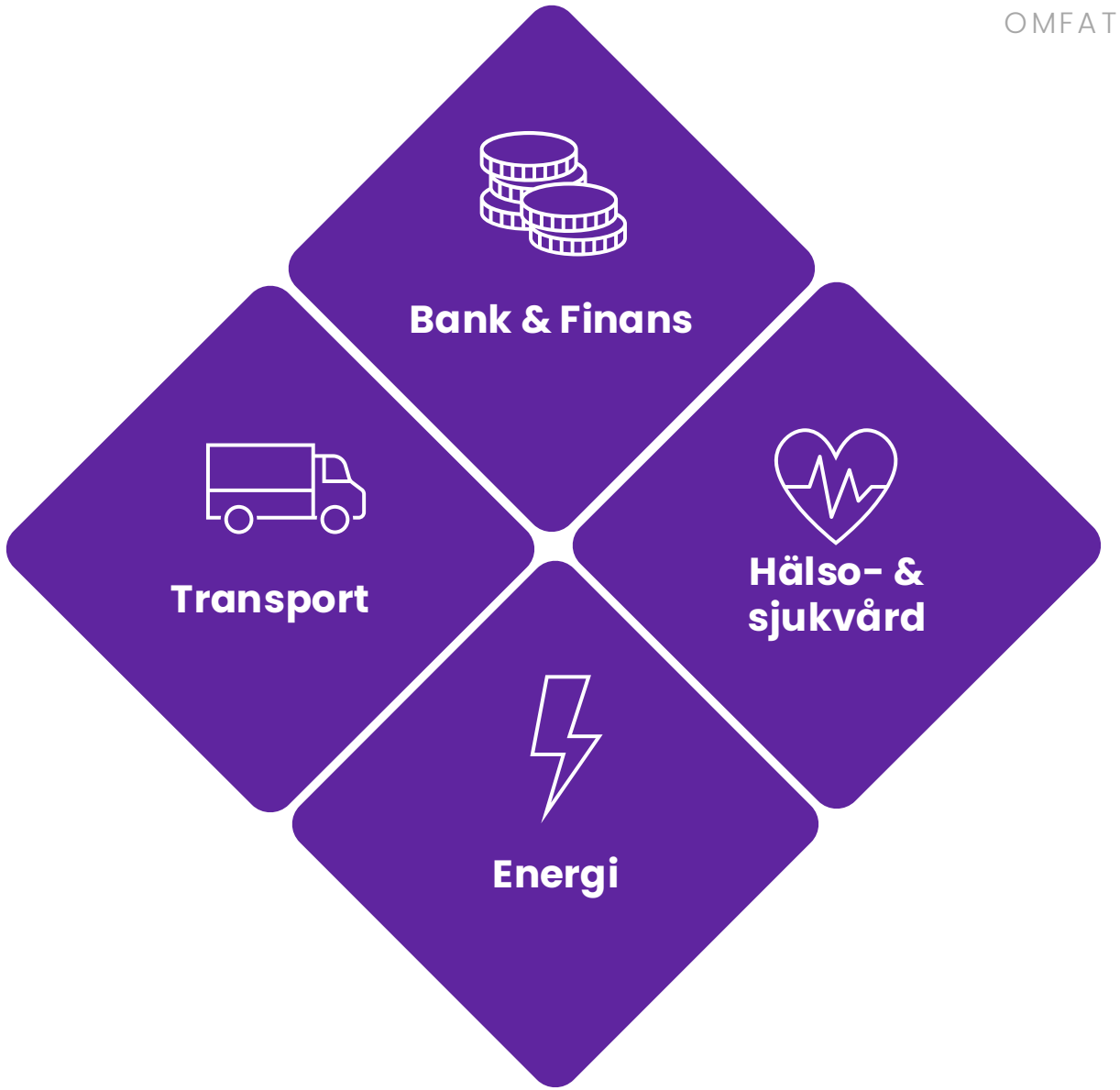
OMFATTNING

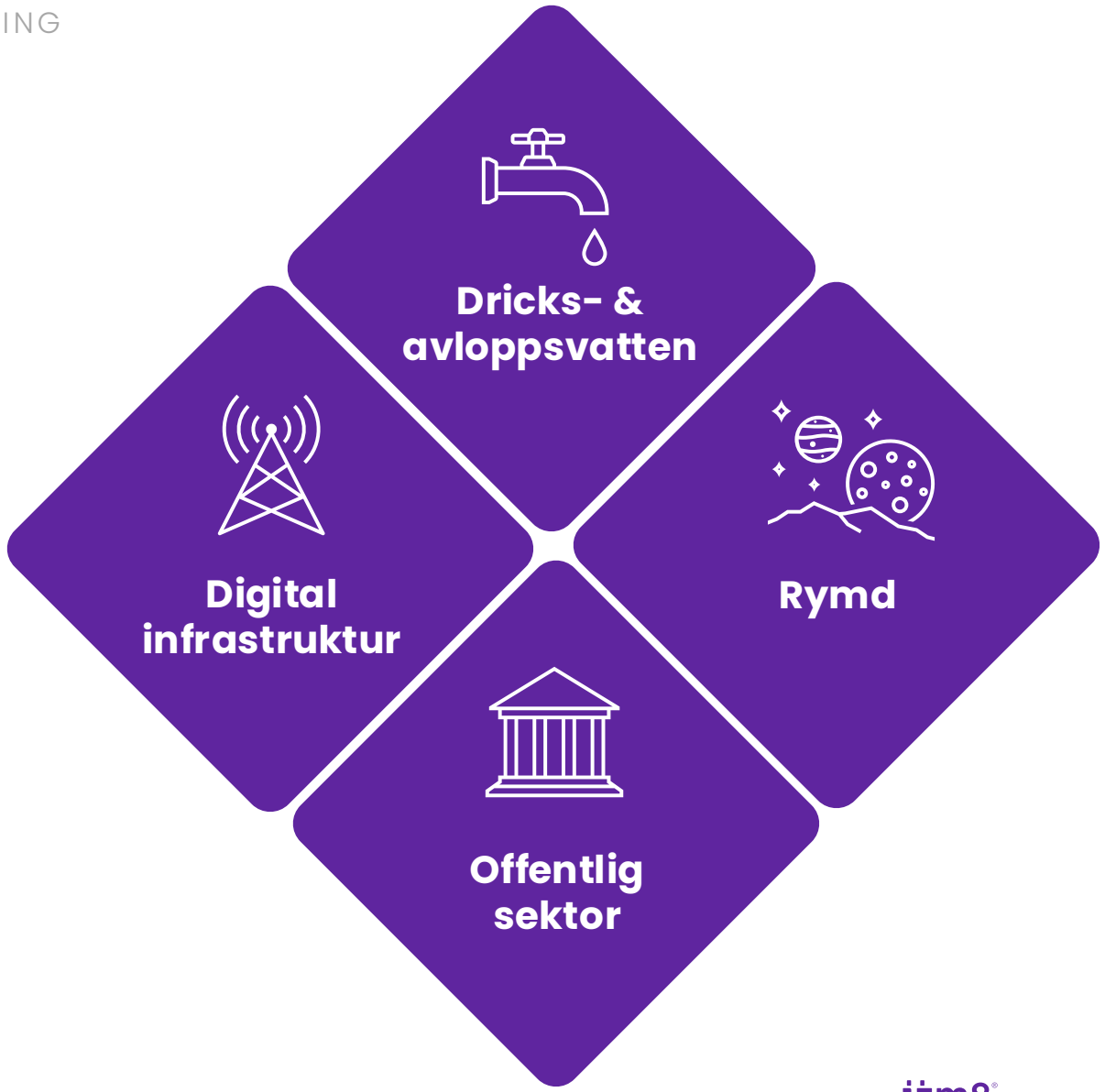




VÄSENTLIGA ENTITETER

OMFATTNING



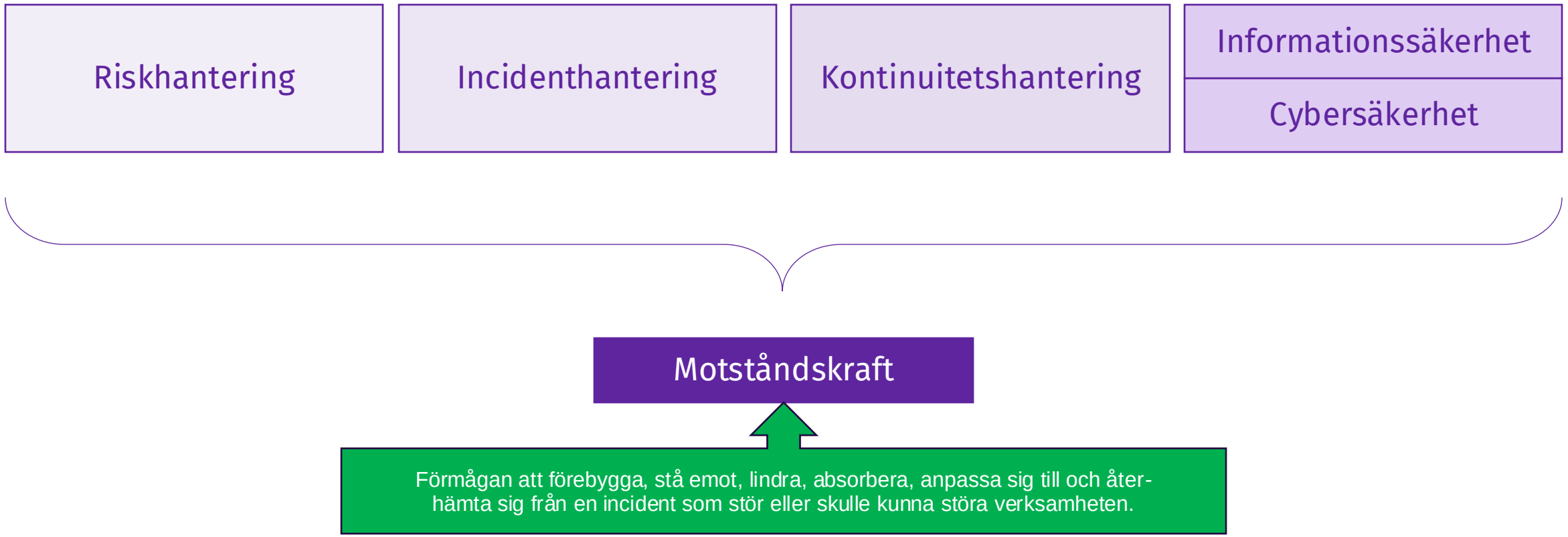


itm8

VAD VILL EU UPPNÅ?

EN BASPLATTA

4 GRUNDLÄGGANDE OMRÅDEN



EN BASPLATTA

4 GRUNDLÄGGANDE OMRÅDEN

Riskhantering

Incidenthantering

Kontinuitetshantering

Informationssäkerhet

Cybersäkerhet

…hantera de risker som kan påverka verksamheten genom att systematiskt identifiera, analysera, utvärdera och behandla risker.

EN BASPLATTA

4 GRUNDLÄGGANDE OMRÅDEN

Riskhantering

Incidenthantering

Kontinuitetshantering

Informationssäkerhet

Cybersäkerhet

…ha en beredskap för att hantera oönskade händelser av olika allvarlighetsgrad när dessa inträffar.

itm8

EN BASPLATTA

4 GRUNDLÄGGANDE OMRÅDEN

Riskhantering

Incidenthantering

Kontinuitetshantering

Informationssäkerhet

Cybersäkerhet

…planera för att kunna upprätthålla verksamhet på en acceptabel nivå, oavsett vilken typ av störning som en organisation utsätts för.

EN BASPLATTA

4 GRUNDLÄGGANDE OMRÅDEN

Riskhantering

Incidenthantering

Kontinuitetshantering

Informationssäkerhet

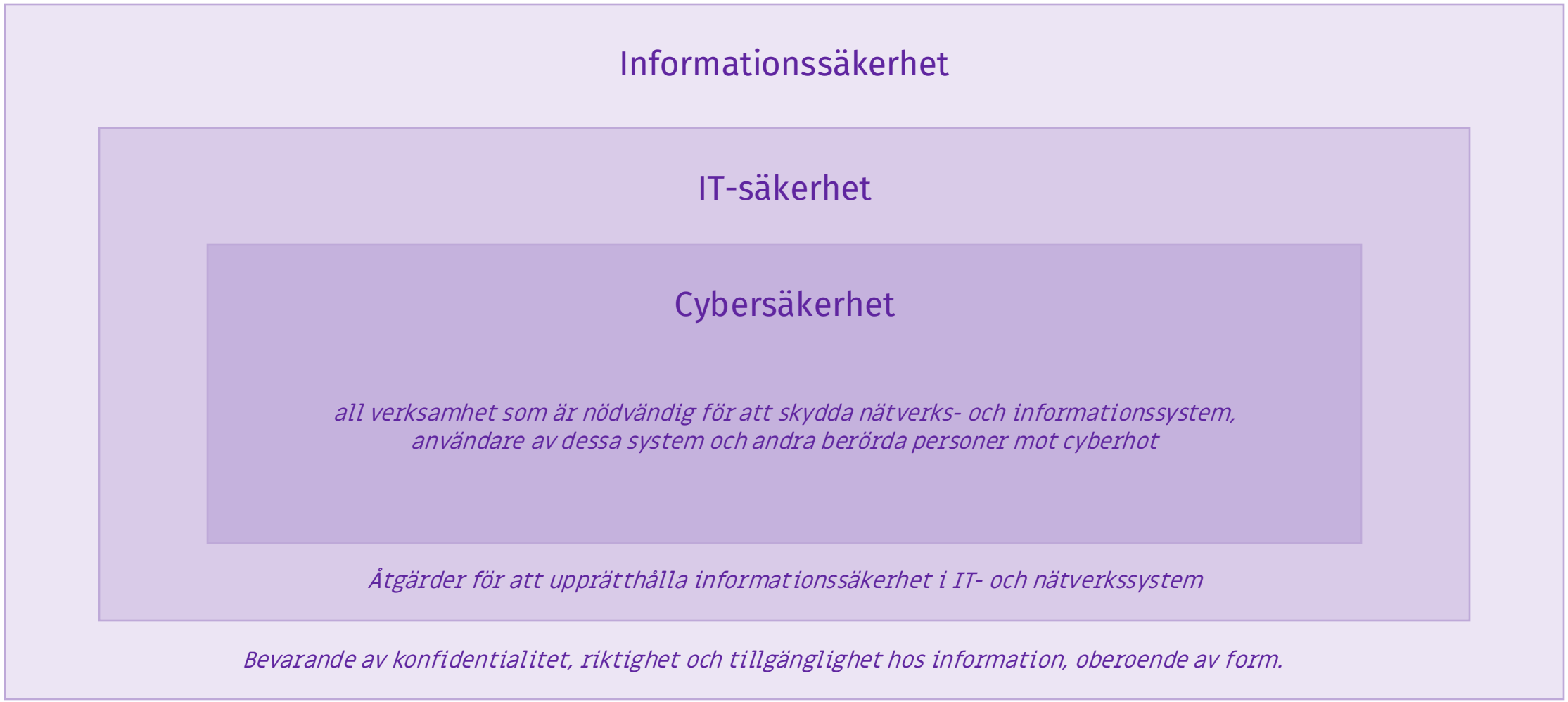
Cybersäkerhet

…skydda information och de informationssystem som behövs för att verksamheten ska fungera.

itm8

INFORMATIONS- & CYBERSÄKERHET

VAD ÄR VAD?



itm8

ATT OMFATTAS, ELLER INTE OMFATTAS…

…DET ÄR FRÅGAN

itm8

OMFATTAS

En verksamhet som faller direkt under de stadgade kategorierna och kriterierna.

Ett bolag som har 50 anställda och/eller omsätter 10 miljoner kronor per år.

Bolaget lever upp till en definition av verksamhet i enlighet med direktivet.

PÅVERKAS

En verksamhet påverkas indirekt genom exempelvis affärsmässiga krav.

Ett bolag som har en kund som omfattas av NIS2 direktivet.

Kunden ställer krav på bolaget att leva upp till specifika krav.

Bolaget kan avfärda kraven. Konsekvensen är affärsmässig, inte legal.

KRITERIER ELPRODUCENT IDAG

KRAV 1

Tjänsten som ni levererar måste vara samhällsviktig såsom beskrivs i MSB:s föreskrift 2021:9

KRAV 2

Verksamheten ska vara etablerad i Sverige

KRAV 3

Leveransen av den samhällsviktiga tjänsten är beroende av ett nätverk- och informationssystem

KRAV 4

En incident i nätverks- och informationssystemet skulle medföra en störning i leveransen av den samhällsviktiga tjänsten

EFFEKTGRÄNS ELLER BALANSRISK

Installerad effekt ska överstiga 30 MW eller så ska avtalet omfatta produktion med balansrisk alt. stödtjänster för nätstabilitet

BALANSANSVAR

Elhandel bedrivs av den med balansansvar enligt ellagen (1997:857)

LEVERANS TILL PRIORITERAD VERKSAMHET

Elproduktionen levererar till verksamheter som är i prioritet 1-5, t.ex. sjukvård, bank och finans, med flera.

CERTIFIKAT

Elöverföring som tillhandahålls av certifierat transmissionsnätsföretag enligt lagen (2011:710) om certifiering av transmissionsnätsföretag för el

itm8

DEFINITION ELPRODUCENT NIS2

Artikel 2.38, EU-direktiv 2019/9442

en fysisk eller juridisk person
som framställer el.

DEFINITION LADDNINGSOPERATÖR NIS2

Bilaga 1, EU-direktiv 2022/2555

Med ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare.

FUNDERINGAR & FARHÅGOR

1

Initiativhämmande

Om solceller blir anledningen till att bolag omfattas kan det påverka viljan att installera sådana; likaså med laddstationer. Detta påverkar i sin tur de interna miljöprojekten och de nationella miljömålen.

2

Otydligt

Osäkerheten kring vad i så fall kommer att anses vara en incident samt som kräver rapportering till en tillsynsmyndighet.

3

Kostnadsdrivande

Säkerheten är viktig oavsett omfattning eller ej, men det går inte att undgå att direktivets omfattning är kostnadsdrivande samt organisationspåverkande.

4

Orimligt

Fastighetsbolag är i regel inte en samhällsviktig aktör; operatörerna i fastigheten kan vara det. Det kan därför tyckas vara orimligt att ett fastighetsbolag ska likställas med ett kärnkraftverk enligt gällande definition.

”VAD BEHÖVER VI GÖRA?”

VÄNTA INTE

1

Hängslen och livrem

Fram tills att detta har förtydligats i lagstiftningen eller genom rättspraxis ska ni utgå från att ni omfattas enligt gällande definition, som en viktig entitet.

2

GAP-analys

Genomför en GAP-analys gentemot kraven för att förstå hur förberedda ni är. Även om det visar sig att ni inte omfattas i framtiden så har ni ett intresse av och krav på er att se över säkerheten.

3

Utgå från ISO/IEC 27001

Utgå från den internationella standarden för att säkra upp verksamheten alternativt från MSB LIS. Ni kommer att ha levt upp till en betydande del av NIS2-kraven genom detta arbete.

GAP-ANALYS

Förberedelse

Gå igenom existerande dokumentation och krav.

Nuvarande status

Analysera hur företaget ligger till redan idag.

GAP

Identifiera de avvikelser från dagens status till krav och mål.

Risker

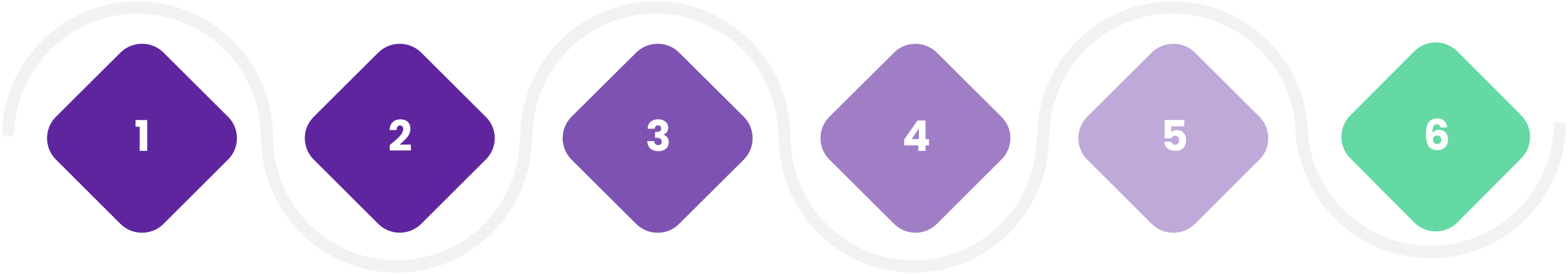
Bedöma och prioritera riskerna utifrån vad som är affärskritiskt.

Åtgärder

Rekommendationer och realistisk åtgärdsplan.

Resultat

Presentera resultat samt nästa steg i processen.



itm8

SÄKERHETSÅTGÄRDER

ETT AXPLOCK

Riskhantering	Incidenthantering	Kontinuitetshantering	Utbildning
Leverantörskedjan	Behörighets- & accesskontroll	Autentisering	Policy & Processer

itm8

”VAD HÄNDER OM VI INTE OMFATTAS I FRAMTIDEN?”

TAR DU AV DIG BILBÄLTET NÄR DU KÖR IN I ETT LAND SOM INTE HAR KRAVET?

FÖRDELAR

1

Juridik

Förberedelse inför framtida krav

Regler och direktiv som NIS2 kan komma att ändras, och att redan ha en planerad strategi sparar tid och resurser om ni plötsligt omfattas.

2

Ekonomi

Minskade konsekvenser vid incidenter

Att identifiera gap och vidta åtgärder innan något inträffar minskar både kostnader och tiden det tar att återställa verksamheten efter en störning.

3

Affär

Ökad konkurrenskraft

Genom att arbeta strukturerat med säkerhet och kontinuitet kan ni positionera er som ett ledande bolag i branschen och attrahera både kunder och investerare.

4

Förtroende

Stärk förtroendet hos kunder och samarbetspartners

En stark säkerhetsprofil visar att ni tar informationssäkerhet på allvar, vilket kan stärka ert rykte och era relationer med hyresgäster och affärspartners.

TACK

SHADI DOMAT

shadi.domat@itm8.com

itm8