Välkomna!

Informationssäkerhetskultur

Tobias Ander

SECURE BY ME
WE

Informationssäkerhetskultur

SECURE BY ME
WE

Tobias Ander

48 år

3 barn

Drygt 20 år inom informationssäkerhetsområdet

- Informationssäkerhetskonsult 2002-2007
- Informationssäkerhetsansvarig 2007-2012
  - Vägverket/Transportstyrelsen
- CISO 2012-2018
  - Transportstyrelsen
- CISO 2018-2023
  - Örebro kommun
- IT-säkerhetschef 2023 →
  - Försvarsmakten (FMTIS)
- Ordf. Kommunfullmäktige 2022 →
  - Lekebergs kommun
- Eget bolag 2021 →
  - Securebyme AB

ÅRETS GRC-PROFIL

Hur vet vi att allting är bra?

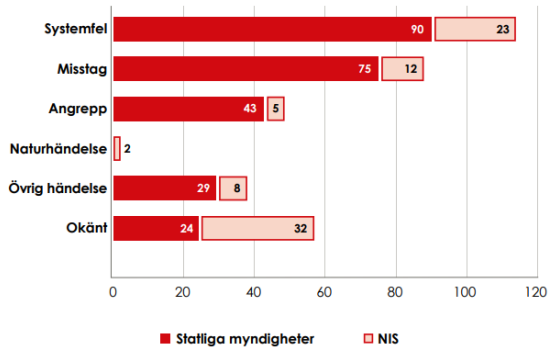
- Huvudsyftet med informationssäkerhet är att undvika eller kontrollera incidenter.

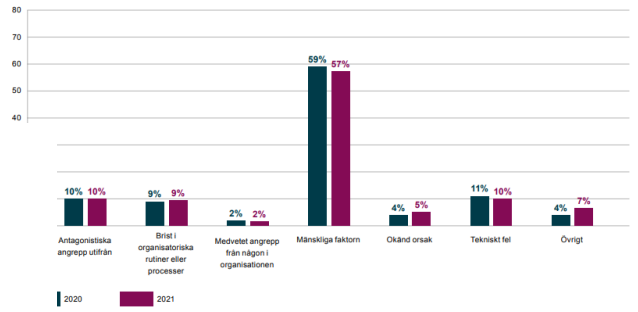
- MSBFS 2020:6
  ” Myndigheten ska ha **förmåga att** skyndsamt upptäcka och bedöma incidenter och avvikelser”

Tre av tio statsanställda fruktar repressalier om de framför kritik

STATSFÖRVALTNING | 2021-12-06

Diagram 2. Antal incidenter 2021 fördelade på orsak.



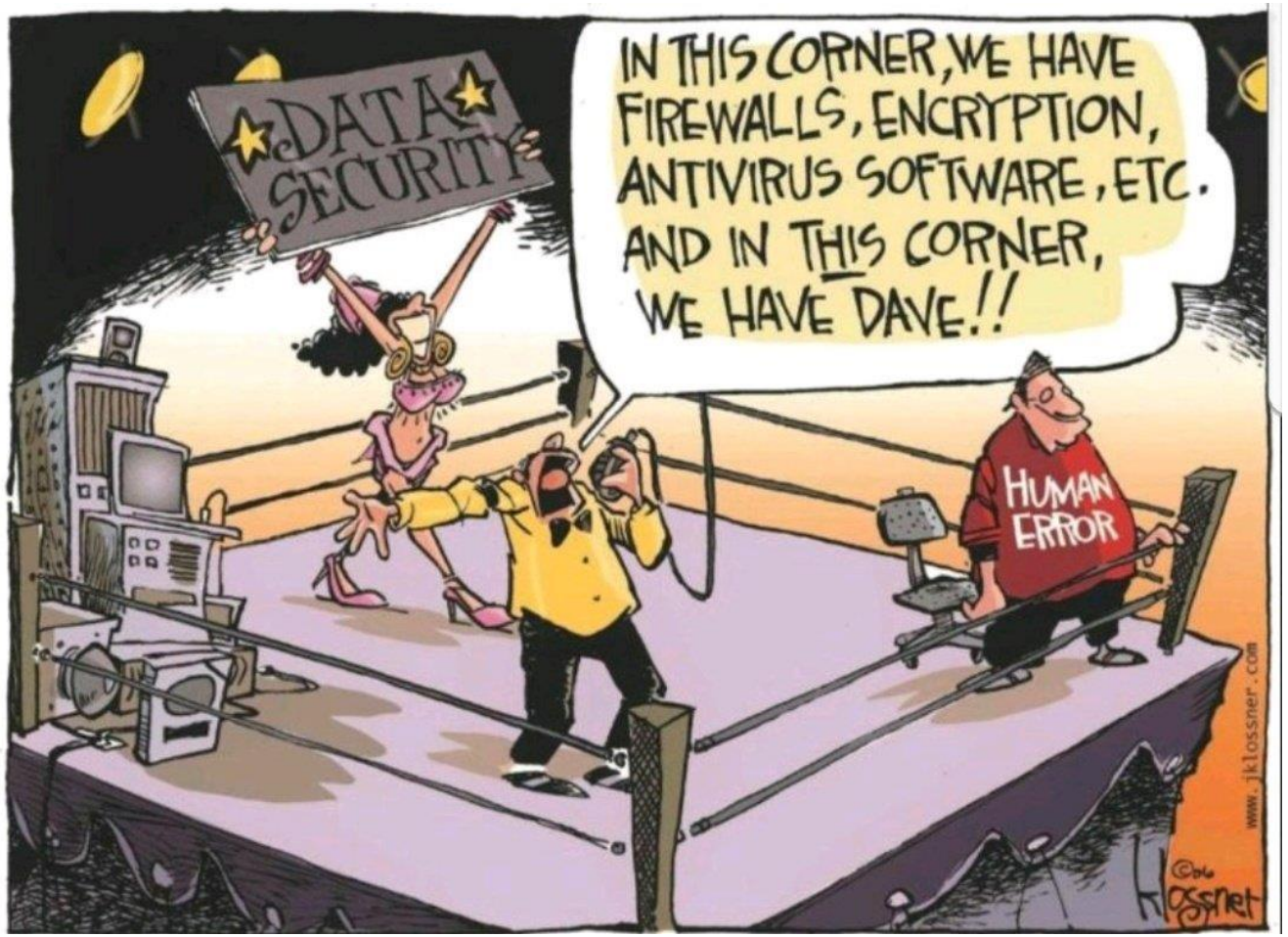


Figur 5. Andel av anmälda personuppgiftsincidenter fördelat på orsak 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

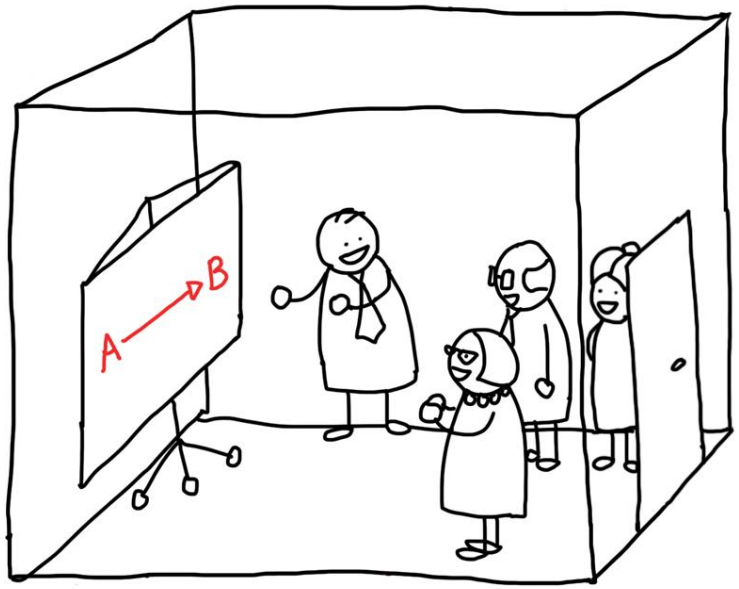
Skandalen, som snabbt kom att kallas ”dieselgate”, briserade **2015**. Då avslöjades att biljätten **Volkswagen** medvetet fuskat och gjort att deras dieselbilar visade upp betydligt mindre utsläpp av kväveoxid än vad de i själva verket släppte ut. 16 sep. 2021

https://www.svt.se › nyheter › utrikes › det-har-ar-volksw...

Det är användarnas fel…

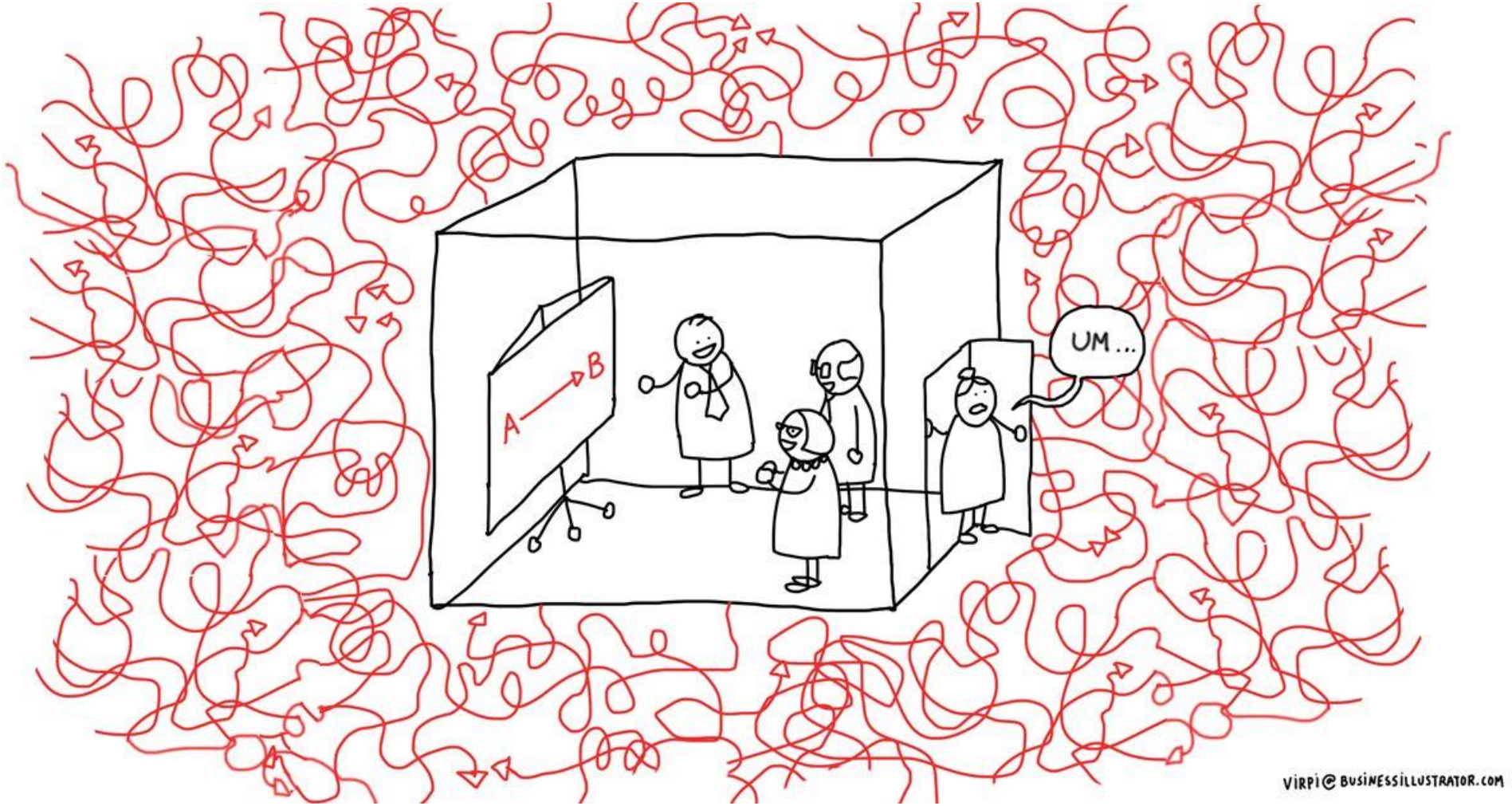


Hur vi driver förändring



VIRPI/BUSINESSILLUSTRATOR.COM

Komplicerat eller komplext



Komplicerade miljöer

- Svåra att förstå sig på
- Lösbara o förutsägbara om man har kunskap om ingående komponenter och deras inbördes relationer
- Ofta i grunden en form av mekniska problem, ex maskiner, datorer designade av människan.

Löses oftast genom att t.ex.

- Ta in rätt expert, göra en modell över systemet, implementera en strategi
- Top –Down förhållningssätt

Komplexa miljöer

- Består avmånga, många delar
- Kännedom och kunskap om ingående komponenter och deras inbördes relationer räcker inte till för att förstå hela systemets egenskaper.
- Kan modeleras till viss del, men inte fullt ut förutsägas.
- Är adaptiva, dvs. förändrar sig när omgivningen förändras, och kan förändra sig själva utan yttre påverkan.

Kan hanteras genom att:

- Finns inga korrekta lösningar!
- Lära sig arbeta kontinuerligt med problemet. (Dansa med det)
- Vara ödmjuk, ompröva beslut och verktyg.

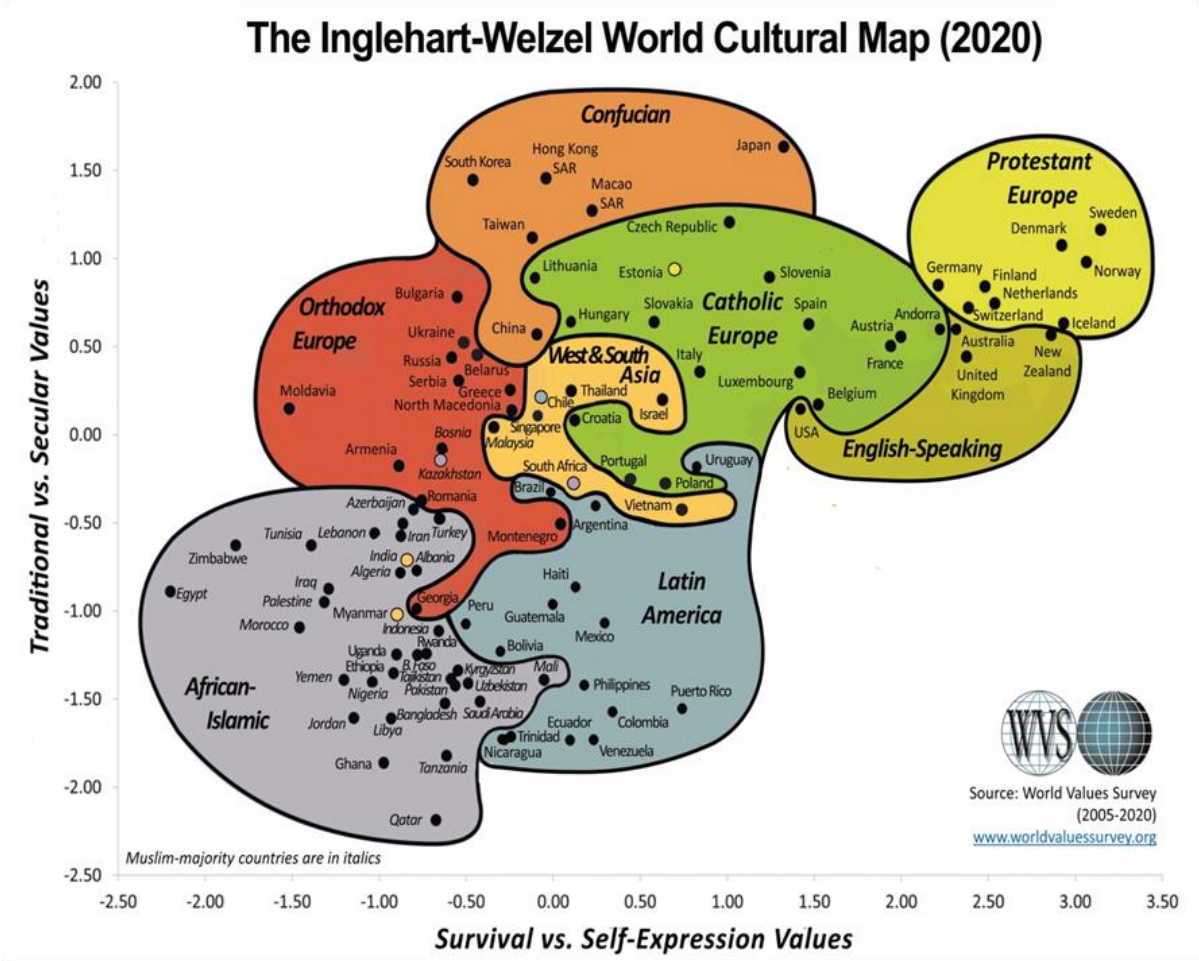
~~Komplicerat~~ – Komplext!

- Vi lever i en allt mer komplex värld, som blir mer och mer oberäknelig och förändras konstant.
- Vi kan då inte bygga en struktur, ett skydd, ett arbetssätt som baseras på logiska samband och fördefinerade värden och information.
- Vi kommer inte bli klara, kunna checka av.
- ”No plan survives contact with the enemy” – Helmuth von moltke

Hur jobbar vi då i en komplex miljö?

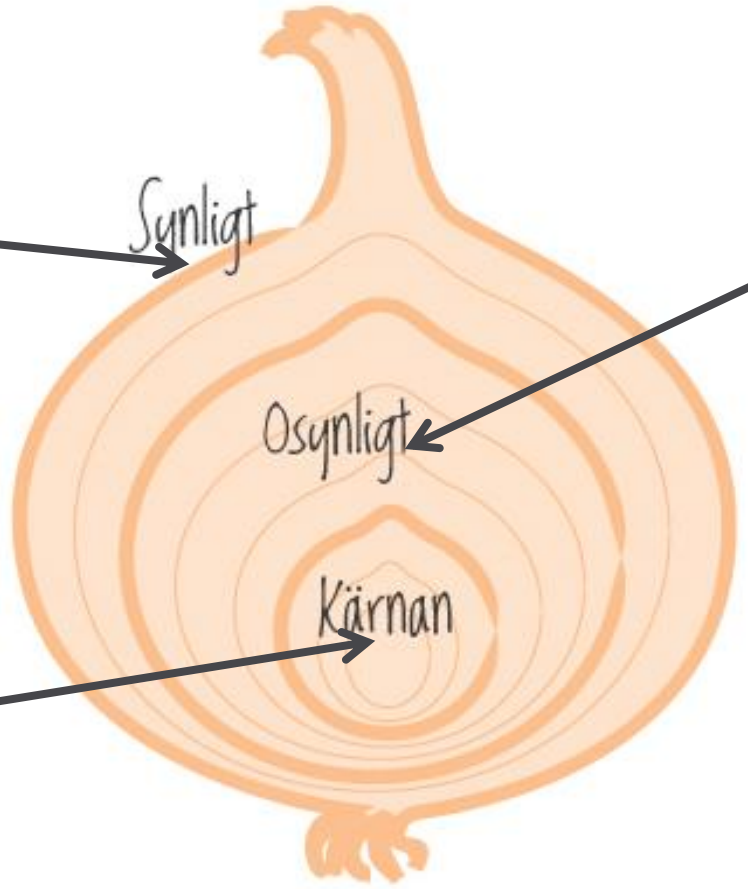
- Mer mandat till de anställda!
  - ”Don’t push information up to authority, push authority down to information” – David Marquet
- Expermintera mera, våga göra fel och dra lärdom!
- Behandla fel och misstag som information och kunskap.
  - ”Avoiding small mistakes makes the big ones more severe” – Nassim Nicholas Taleb
- Uppmuntra informationsdelning och samarbeten.

Kultur i omvärlden



Kultur i en organisation

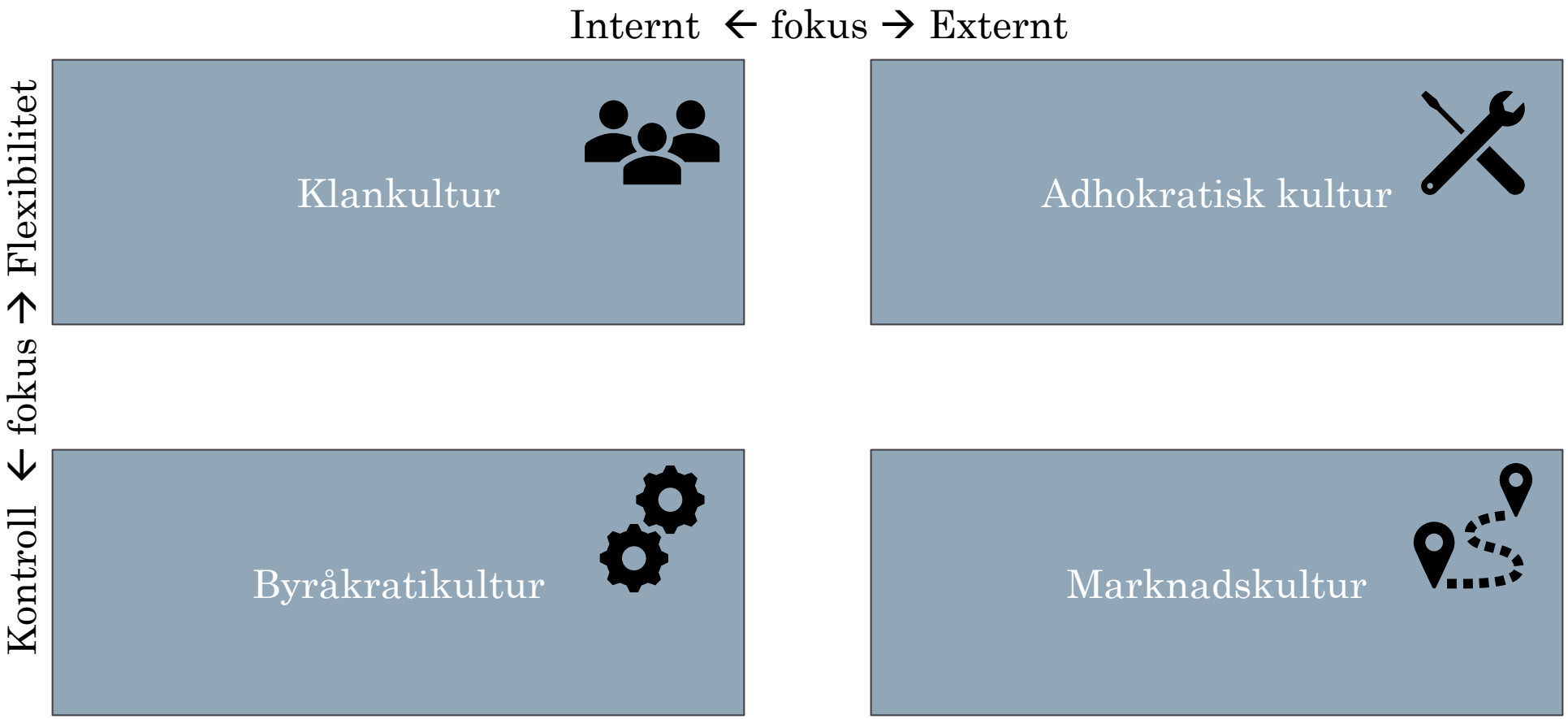
Organisation
Formellt ledarskap
Policy
Ledningssystem
Valda arbetssätt
Dokumenterade rutiner



Nätverk/”stammar”
Informellt ledarskap
Organisatoriska vanor
Värderingar
Attityder
Normer

Vem är jag?
Varför är jag här?
Vad är jag en del av?
Vad hotar min existens?

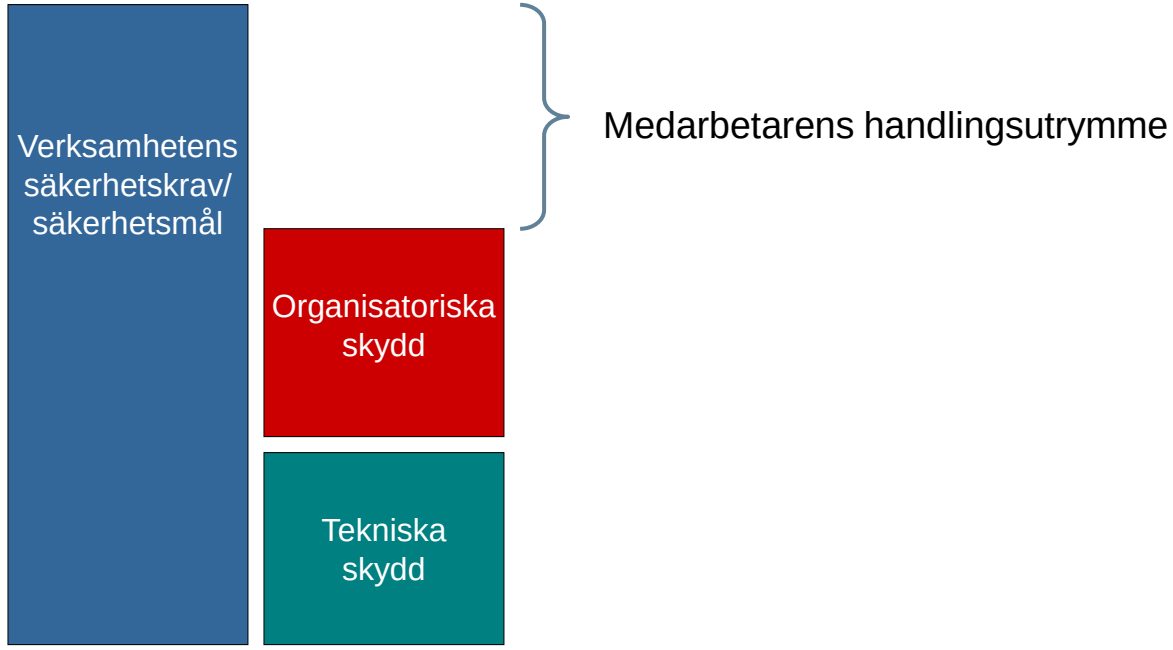
Organisationskulturer



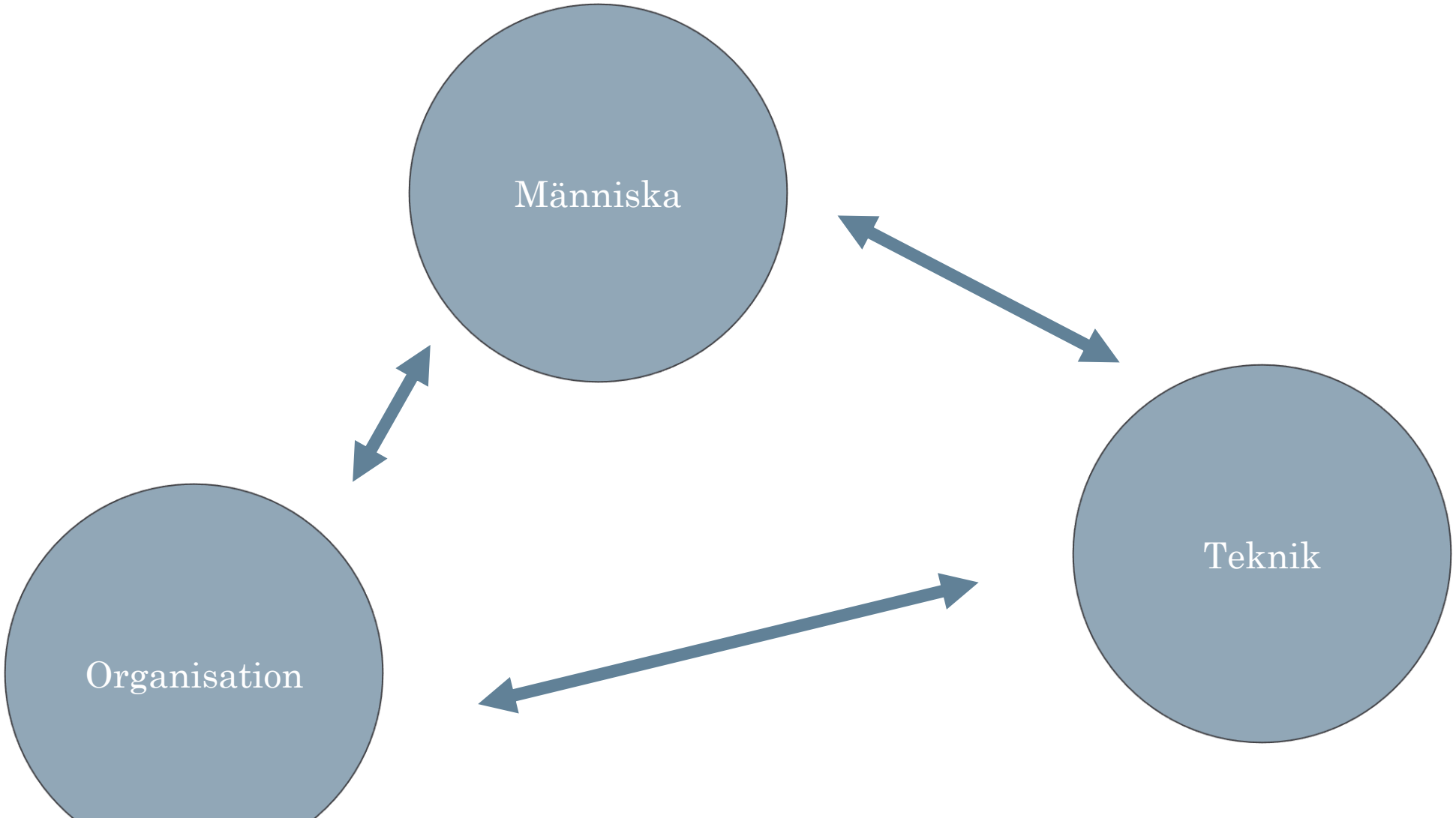
Informationssäkerhetskultur

Informationssäkerhetskultur handlar om en organisations gemensamma sätt att tänka och agera i förhållande till risk och informationssäkerhet, dvs. hur en organisation prioriterar och faktiskt arbetar med risker och informationssäkerhet kopplat till sin verksamhet.

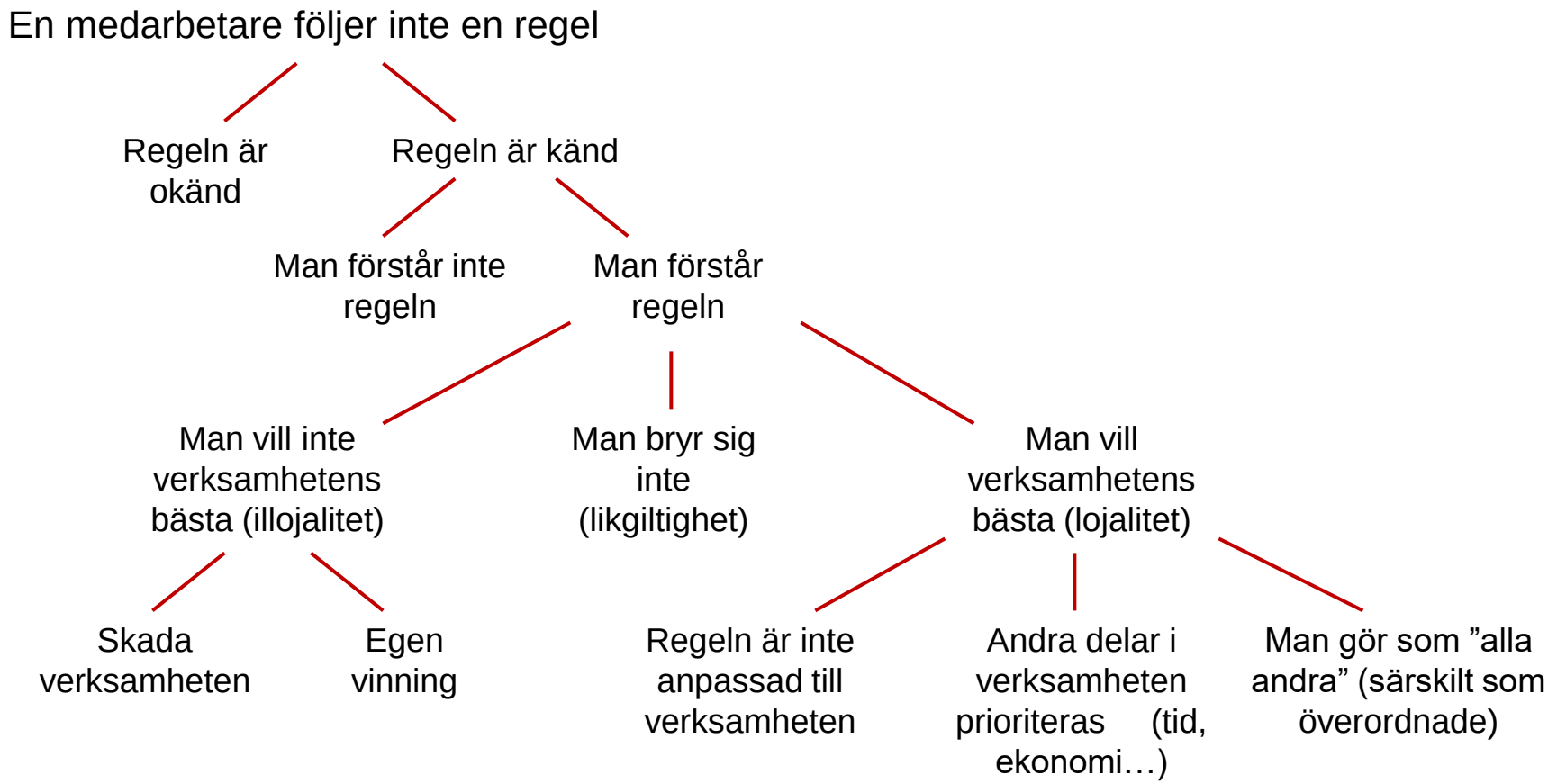
Medarbetarnas utrymme



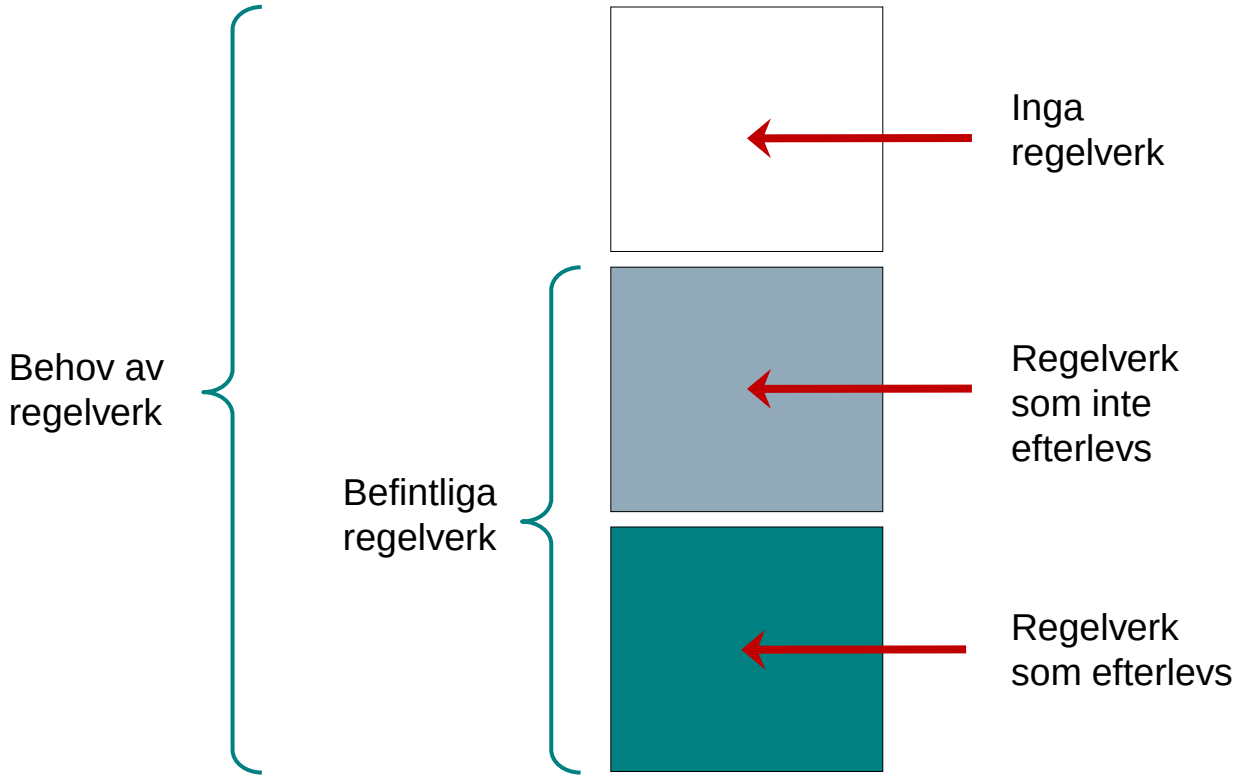
Att förlita sig bara på teknik



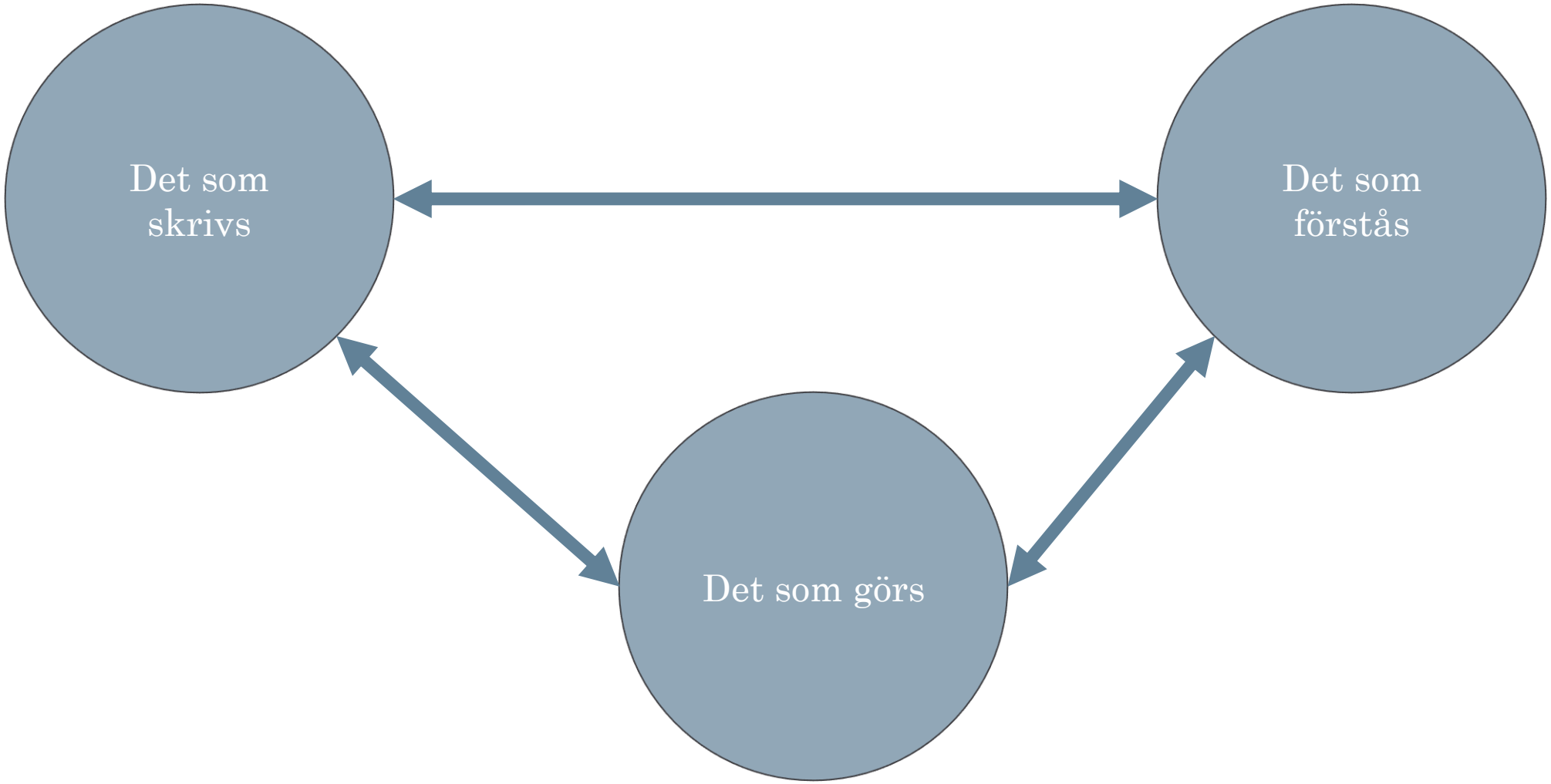
Regler som inte efterlevs



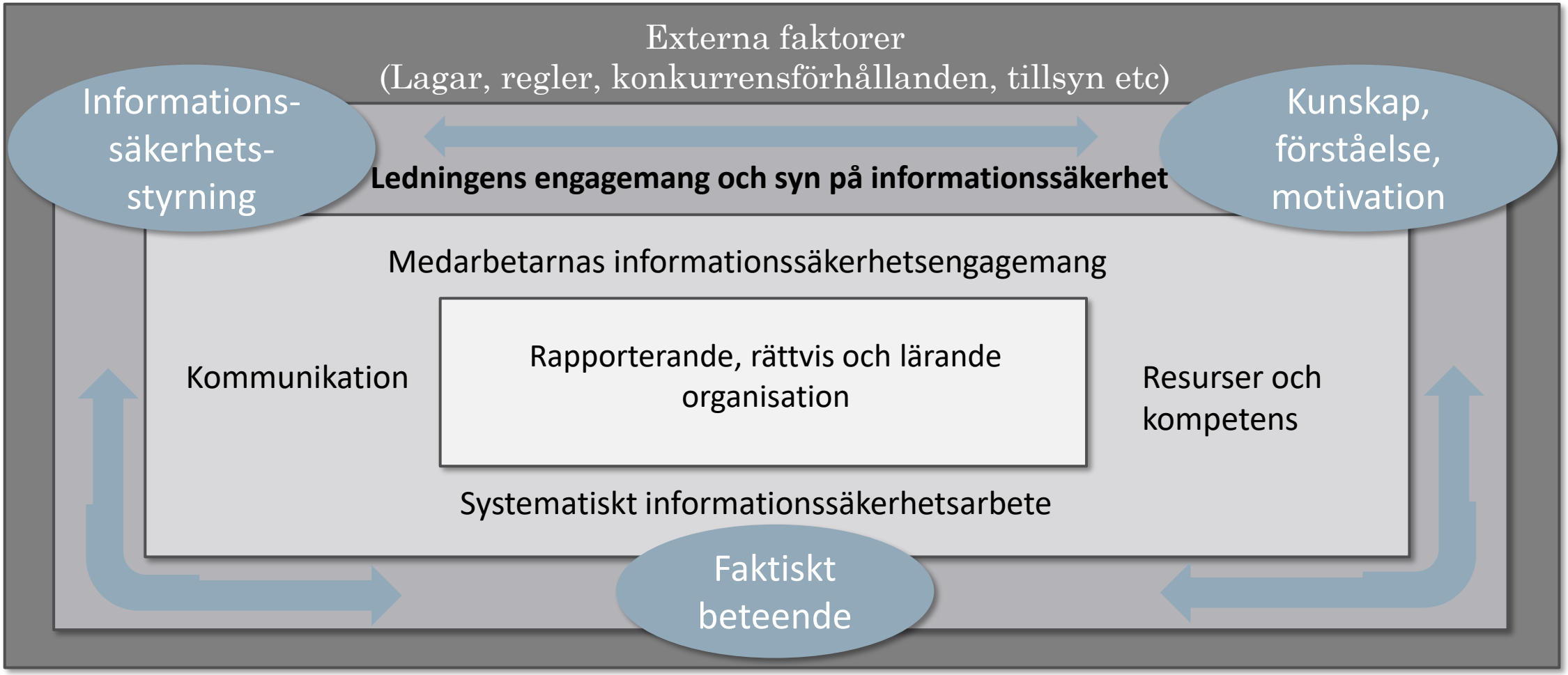
Regelverk eller brist på regelverk



Samverkande element



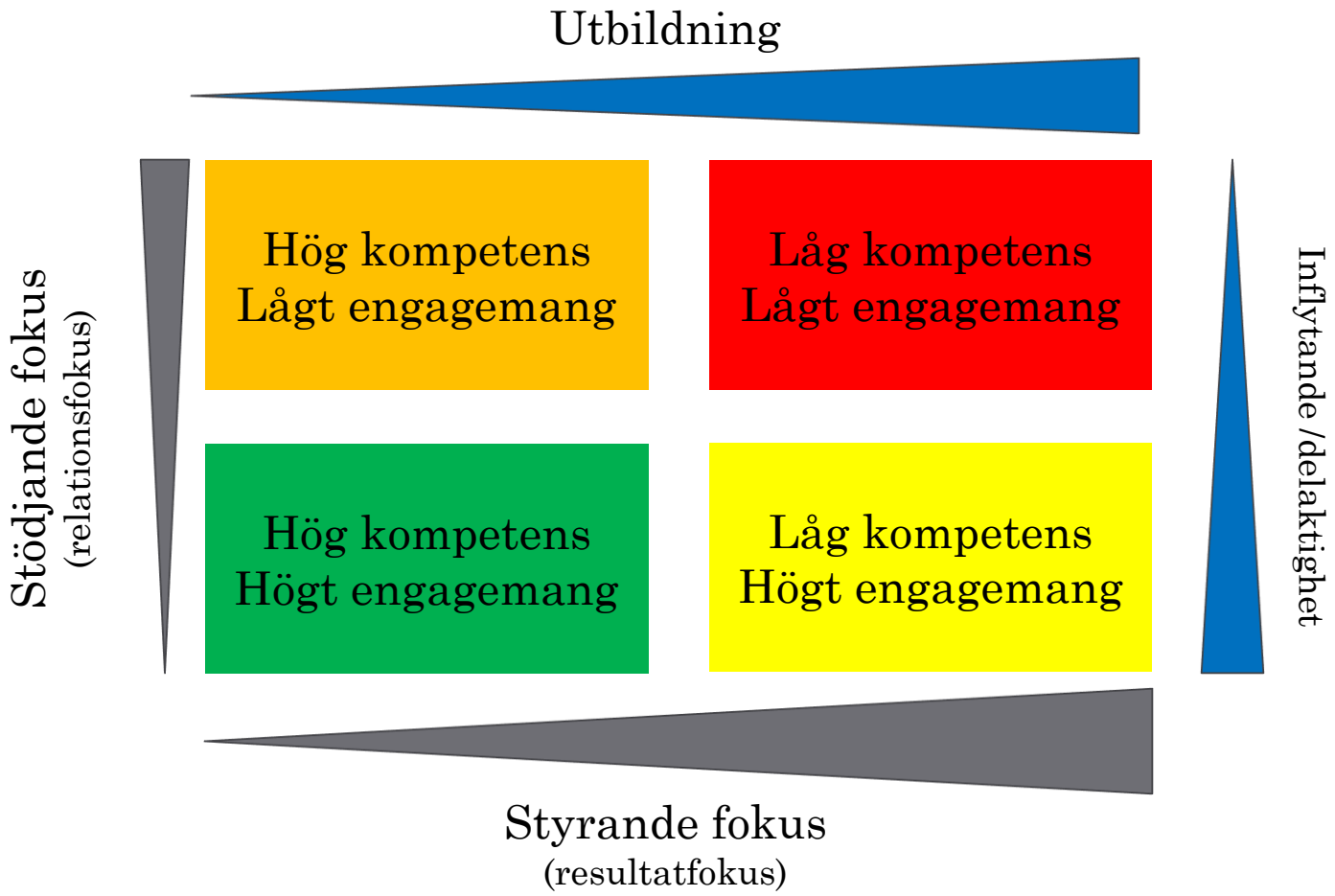
Vilket utrymme har vi för rätt kultur?



Situationsanpassad systematik

Hög kompetens Lågt engagemang	Låg kompetens Lågt engagemang
Hög kompetens Högt engagemang	Låg kompetens Högt engagemang

Situationsanpassad systematik



Psykologisk trygghet

- På en psykologiskt trygg arbetsplats hindras medarbetare inte av social rädsla. De vill och vågar ta inneboende sociala riskerna som öppenhet innebär. De är mer rädda för att inte delta helhjärtat än för att dela med sig av en idé även om den kan vara känslig, hotfull eller helt enkelt fel.

- **Medarbetare vill och vågar ta sociala risker som öppenhet innebär.**

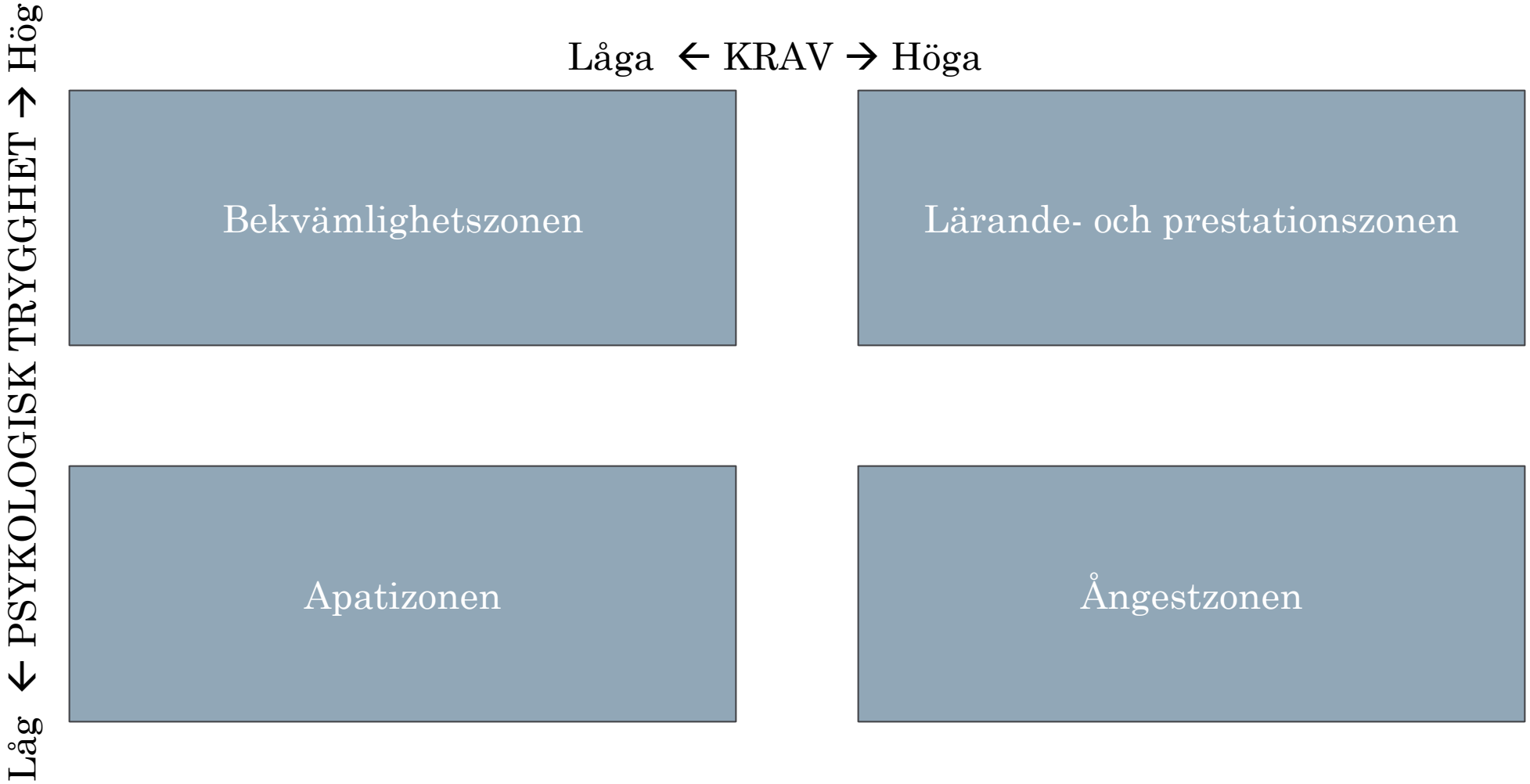
- Det innebär att:

- **Dagens ledare måste vara villiga att anta uppgiften att utplåna rädsla ur organisationen för att skapa de rätta förhållandena för lärande, innovation och tillväxt.**

Psykologiskt trygga grupper

- Psykologiskt trygga grupper gör färre misstag och berättade oftare om de misstag som ändå gjordes. Psykologisk trygghet byggs upp av gott ledarskap (exempelvis gruppledare tydligt visar att de prioriterar säkerhet och öppenhet) ihop med en tydlig, delad förståelse för att arbetet är komplext och kräver samarbete. **Den psykologiska tryggheten ger, i sin tur, en ökad ärlighet, som är helt avgörande för att säkerställa god säkerhet idag.**

Effekten av krav och psyk. trygghet.



Ledares två viktigaste uppgifter

- De måste skapa psykologisk trygghet som främjar lärande, och motverkar misslyckanden som går att undvika.

- De måste ställa höga krav och inspirera och hjälpa medarbetarna att uppfylla dem.

En ledare behöver även

- En ledare måste vara villig att vara sårbar och öppen med sina egna misstag, så att andra känner sig trygga.

- Om du som ledare tror att du har alla svar, sluta med det. För du kommer ha fel!

Att driva förändring

Varför

- Vad är syftet och målet och varför ska jag ändra mig?

- **Kommunicera**
- **Ledningsgruppens engagemang**
- **Utbildning och stöd till chefer och ledare**
- **Begriplig, tillgänglig information.**

Vilja

- Att vara en del i utvecklingen

- **Synligt ledarskap**
- **Delaktigt och förberett ledarskap**
- **Identifiera risker och hinder**
- **Att engagera berörda medarbetare**
- **Belöningsprogram**

Vetskap

- Hur ska jag göra för att förändra mig och vilken attityd är önskvärd?

- **Hur ska förändringen gå till**
- **Vilka beteenden förväntas vi ha**
- **Handböcker, trycksaker och wiki**
- **Samarbetsgrupper**

Förmåga

- Att genomföra förändringen, ändrat sin attityd och beteendekontroll.

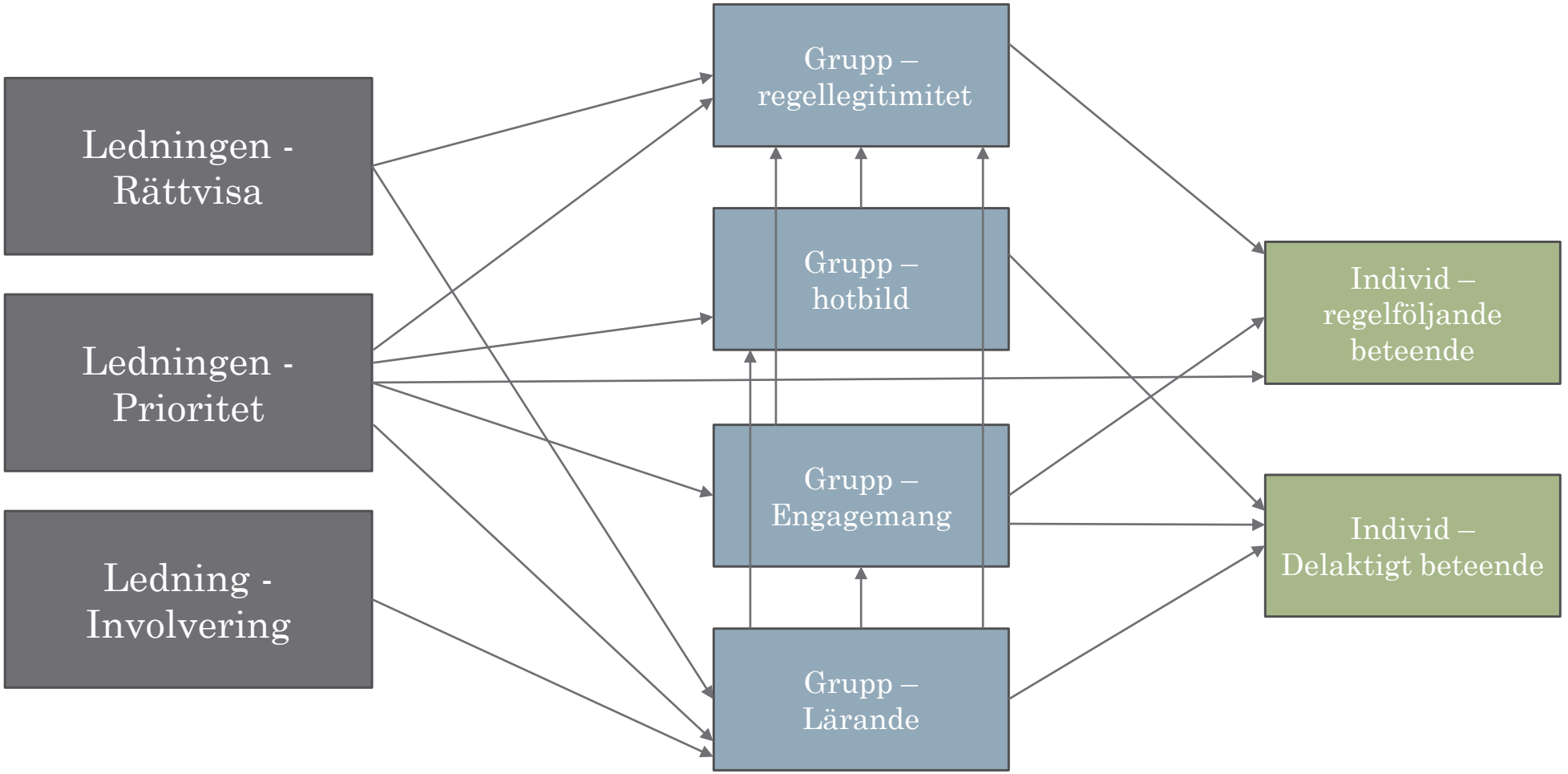
- **Dagligt stöd från chefer och ledare**
- **Expertstöd**
- **Praktiska övningar**
- **Mäta och följa upp**

Förstärka

- Vidmakthålla beteenden så att de inte blir nedprioriterade.

- **Fira och ge beröm**
- **Belöningar och utmärkelser**
- **Återkopplingar från medarbetare**
- **Verksamhetens ansvar**

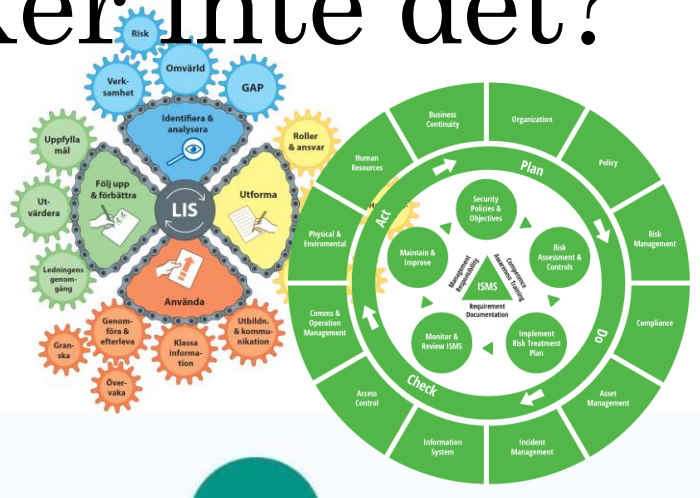
Ledningens betydelse



Mognadsnivåer

- Skapande
  - Alla nivåer i organisationen deltar
  - Informationssäkerhet är en naturlig del
  - Är orolig för att bli självbelåtna
- Proaktiv
  - Medarbetarna tar egna initiativ
  - Inte beroende av att högsta ledningen styr arbete
- Planerande
  - LIS finns
  - Högsta ledningen styr arbetet
- Reaktiv
  - Agerar efter incidenter skett
  - Börjar ta fram rutiner och struktur
- Sjuklig
  - Inte få anmärkning
  - Medarbetarna är problemet

Men vi har ju ett LIS räcker inte det?

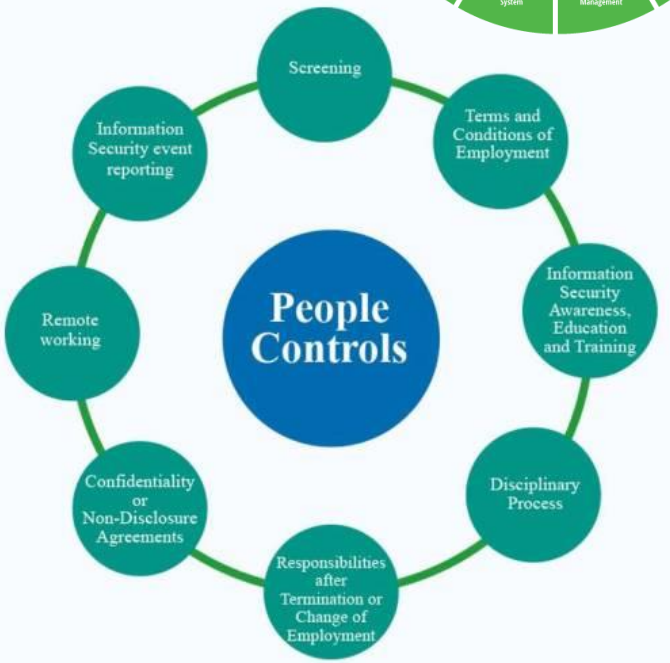


Ett formellt Ledningssystem för Informationssäkerhet (LIS) är inte tillräckligt.

Det leder inte automatiskt till en god säkerhetskultur

En god informationssäkerhetskultur är en förutsättning för ett effektivt LIS

Men ett effektivt LIS gynnar utveckling av en god informationssäkerhetskultur



Exempel på böcker

- Cyber Security Culture – Peter Trim, David Upton
- Build a Security Culture – Kai Roer
- People-Centric Security – Lance Hayden
- Transformational Security Awareness – Perry Carpenter
- The Psychology of information security – Leron Zinatullin
- The Security Culture Playbook – Kai Roer, Perry Carpenter
- Cybersecurity culture in organizations – Isabella Corradini

- **Informationssäkerhetskultur en handbok – Tobias Ander**

”

I det FMTIS som jag leder, talar man öppet och ärligt om sina framgångar men också om sina misstag, i syfte att lära av varandra.

Överste Magnus Tillby
Förbandschef FMTIS

Tack för idag!

Tillsammans gör vi skillnad!

- www.linkedin.com/in/tobiasander
- https://www.securebyme.se
- tobias@securebyme.se

SECURE BY ME