

Agilt arbetssätt och informationssäkerhet

SAFe vs ISO 27001

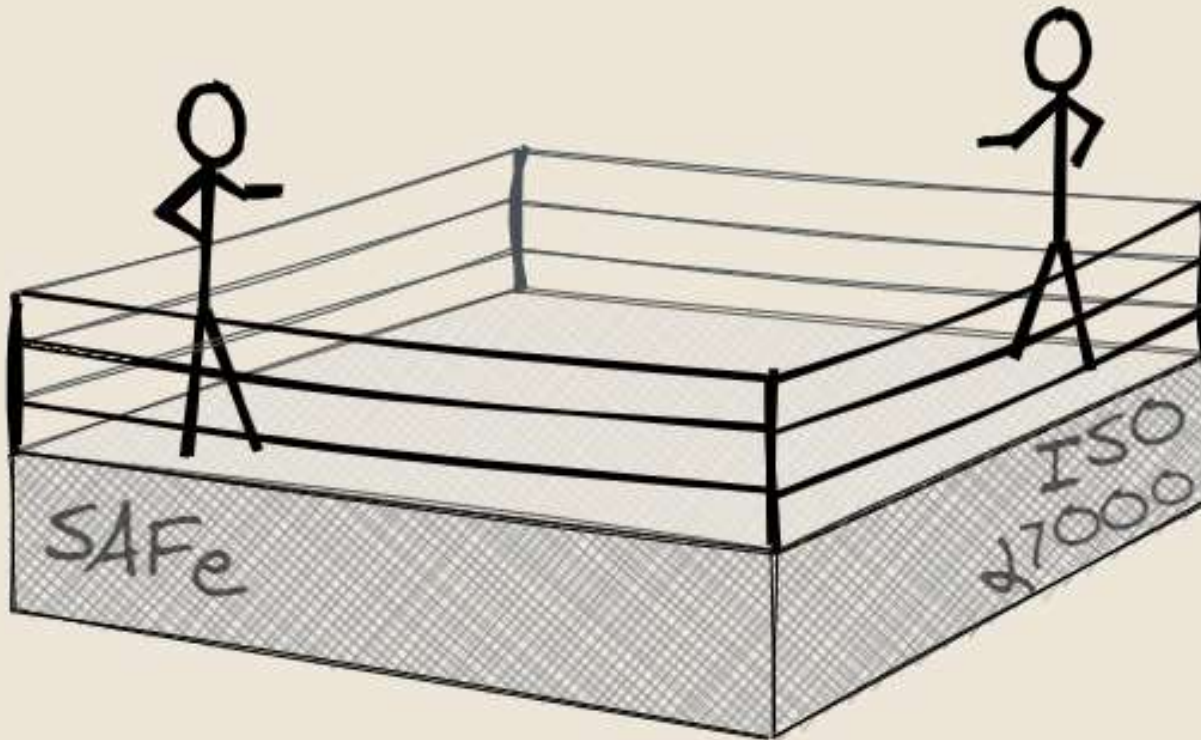
"Risk comes from not knowing what you're doing." — Warren Buffett



Ulf Dellborg

- Flygsäkerhet Viggen FV/FMV
- Signalsystem Adtranz
- Kunsult IT++
 - Projektledning
 - Krav
 - Arkitektur
 - Säkerhet

Agilt vs Informationssäkerhet!



Syfte

- Förstå säkerhet & agilt

Innehåll

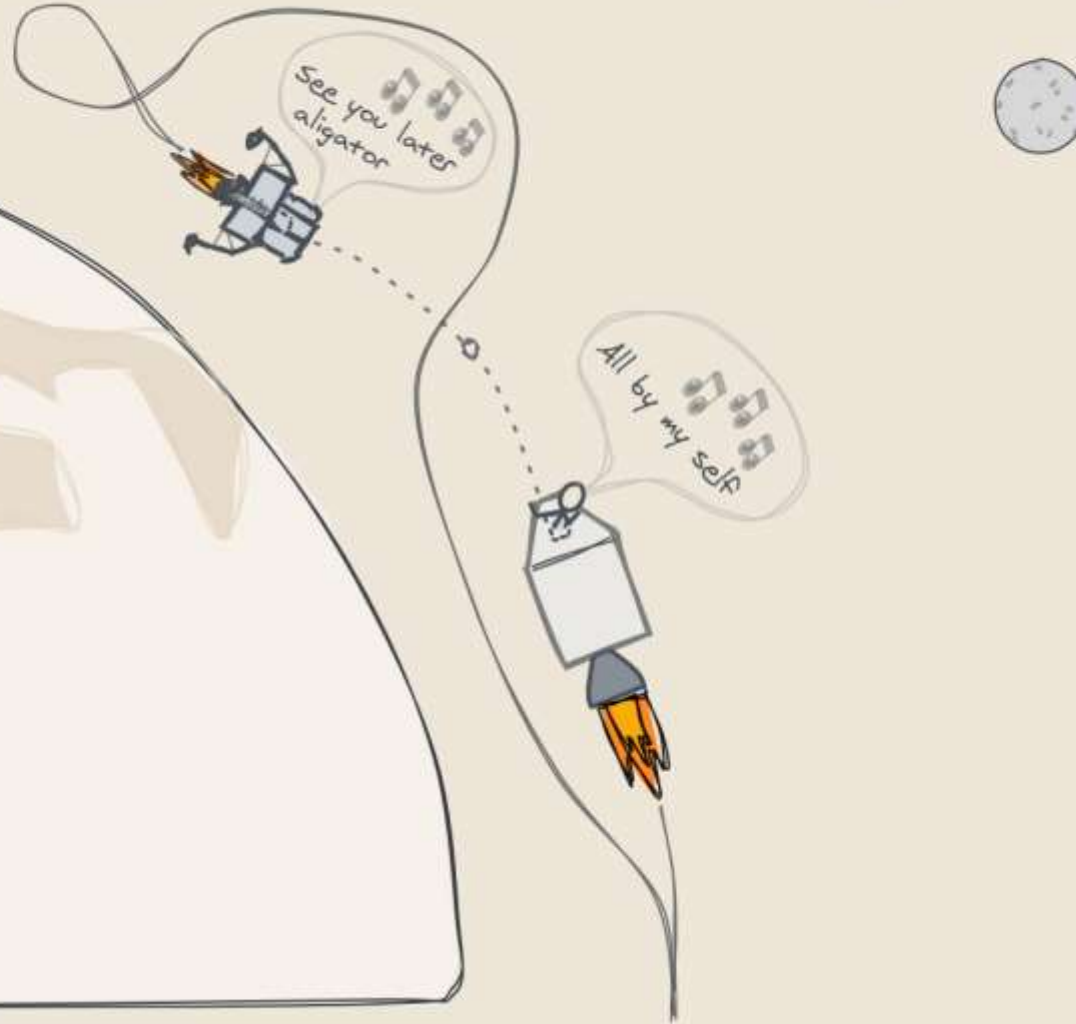
- Säkerhet och utveckling
- SAFe och ISO27001
- Kap 4 Sammanhang
- Kap 5 Ledning
- Kap 6 Planering
- Kap 7 Support
- Kap 8 Operativt arbete
- Kap 9 Utvärdering
- Kap 10 Förbättring

Apollo 8, flyga runt månen



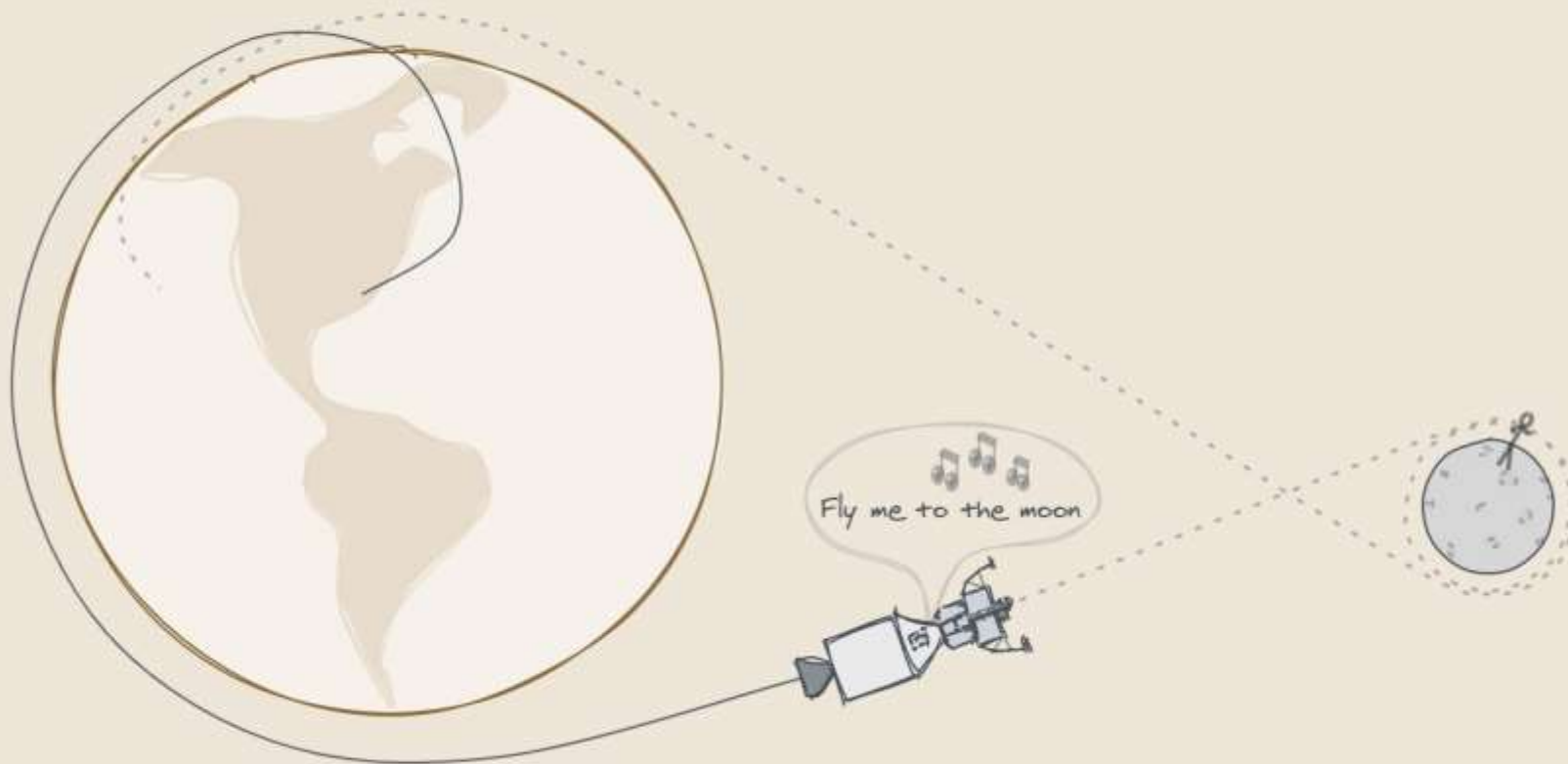
Säkerhet, Agilt, nytt?

Apollo 9, Prova mänlandaren....



Säkerhet, Agilt, nytt?

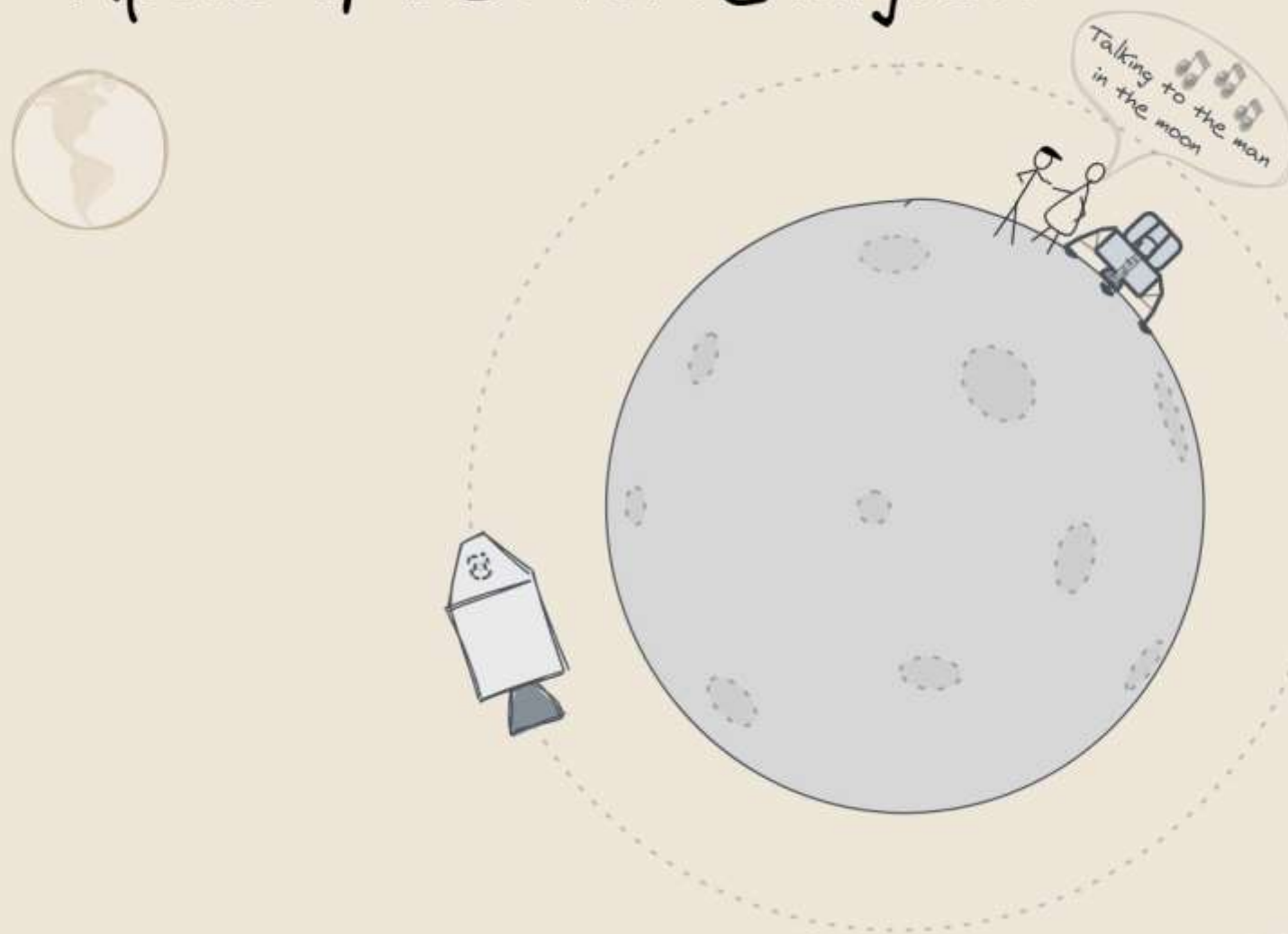
Apollo 10, "dressed rehearsal"



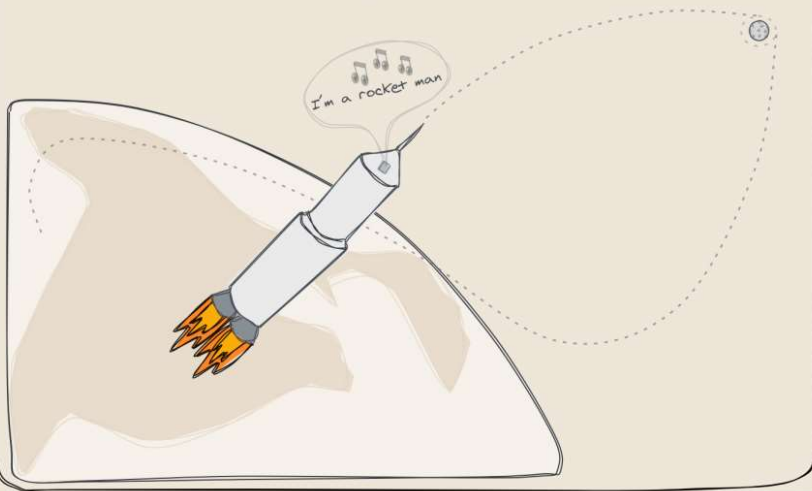
Säkerhet, Agilt, nytt?

Apollo 11, idén förverkligad! 💡

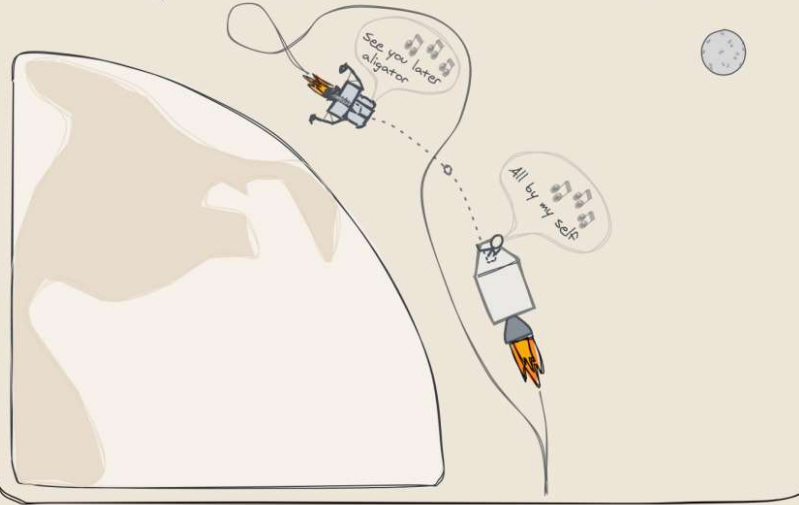
Säkerhet, Agilt, nytt?



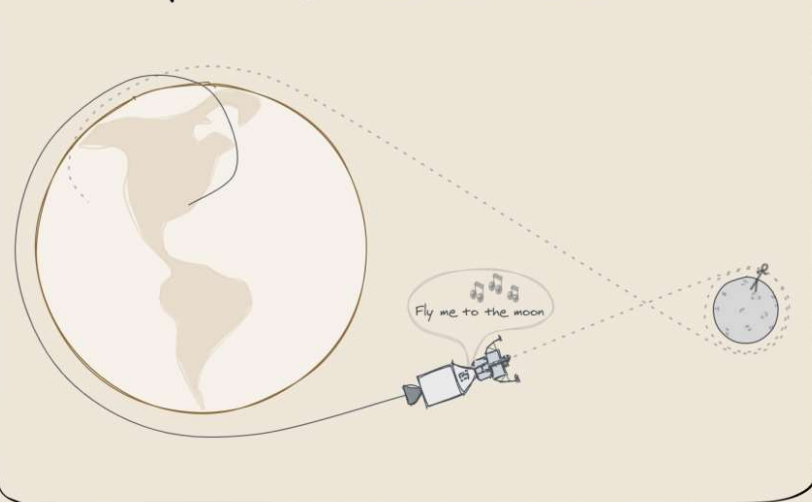
Apollo 8, flyga runt månen



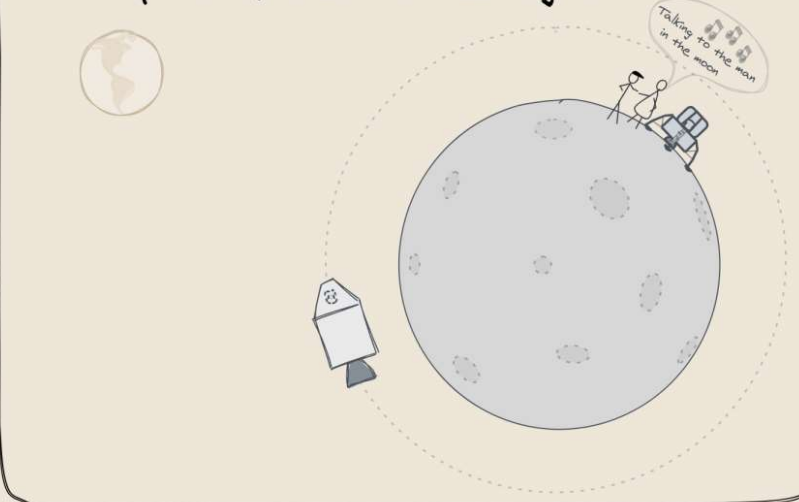
Apollo 9, Prova månlandaren....



Apollo 10, "dressed rehearsal"



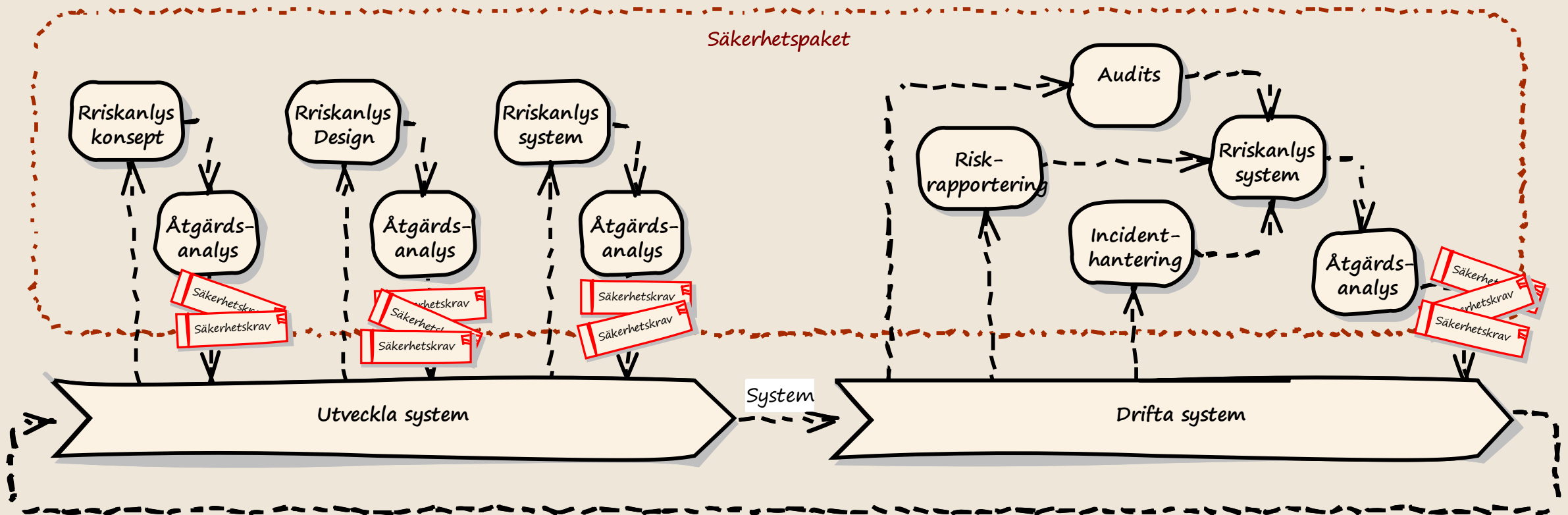
Apollo 11, idén förverkligad!



Säkerhet, Agilt, nytt?

- ANSI/ISA S84 (Functional safety of safety instrumented systems for the process industry sector)
- IEC 61511 (Safety instrumented systems for the process industry sector)
- IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems)
- IEC 60601 (safety and effectiveness of medical electrical equipment)
- IEC 61513 (nuclear industry)
- IEC 62061 (safety of machinery)
- EN 50128 (railway applications – software for railway control and protection)
- EN 50129 (railway applications – safety related electronic systems for signalling)
- EN 50402 (fixed gas-detection systems)
- ISO 26262 (automotive industry)
- MISRA, various (guidelines for safety analysis, modelling, and programming in automotive applications)
- Defence Standard 00-56 Issue 2 – accident consequence
- ISO 27000, 27001, 27002

Säkerhetsmetod, ooops Privacy By Design



SAFe



SAFe, vad jag ser:

Hierarki

- Portfolio, Program, Team

Flöden

- Development value stream, Operational value stream, Solution Train, Continuous Delivery pipeline, Agile Release Train, Program Increments och iterations

Events

- Iteration planning, Daily stand up, Iteration review, Iteration retrospective, PI-planning, Scrum of Scrums, Solution Demo, ART Sync, Portfolio Sync, PO Sync, System Demo, Inspect and Adapt, Lean Budget Review, Communities of Practice, Roadshow

Uppgifts- & kravhantering

- Kanbans, Backlogs, Epics, Epic enablers, Features, Fetaure enablers, Stories & Story enablers

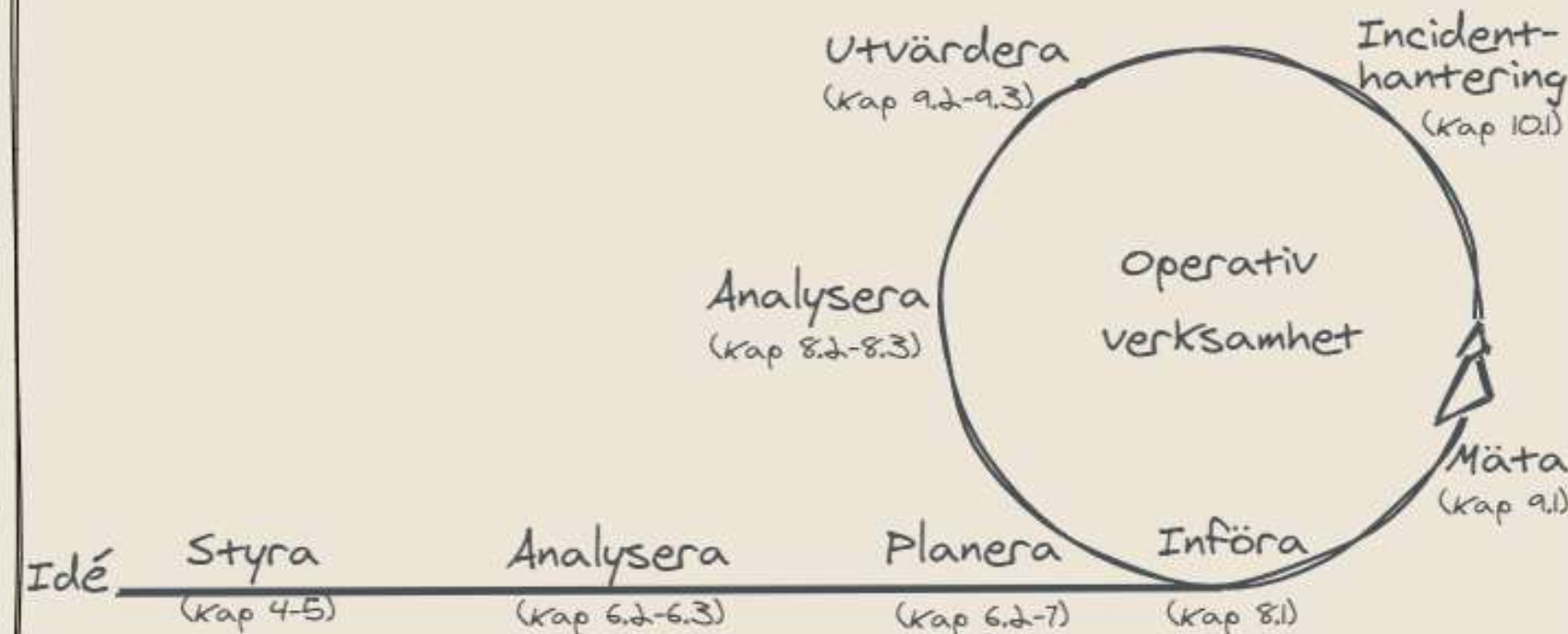
Dokumentation

- Business Canvas, Portfolio Canvas, Development Value Stream Canvas, Agile Release Train Canvas, Portfolio vision, Solution Vision, Solution Intent

Roller & ansvar

- Epic Owners, Enterprice Arhcitect, Solution Architect, Solution Mgmt, STE, Business Owners, System Architect, Product Mgmt, Product owne, DevTeam

ISO 27000 !



Serien ISO 27000

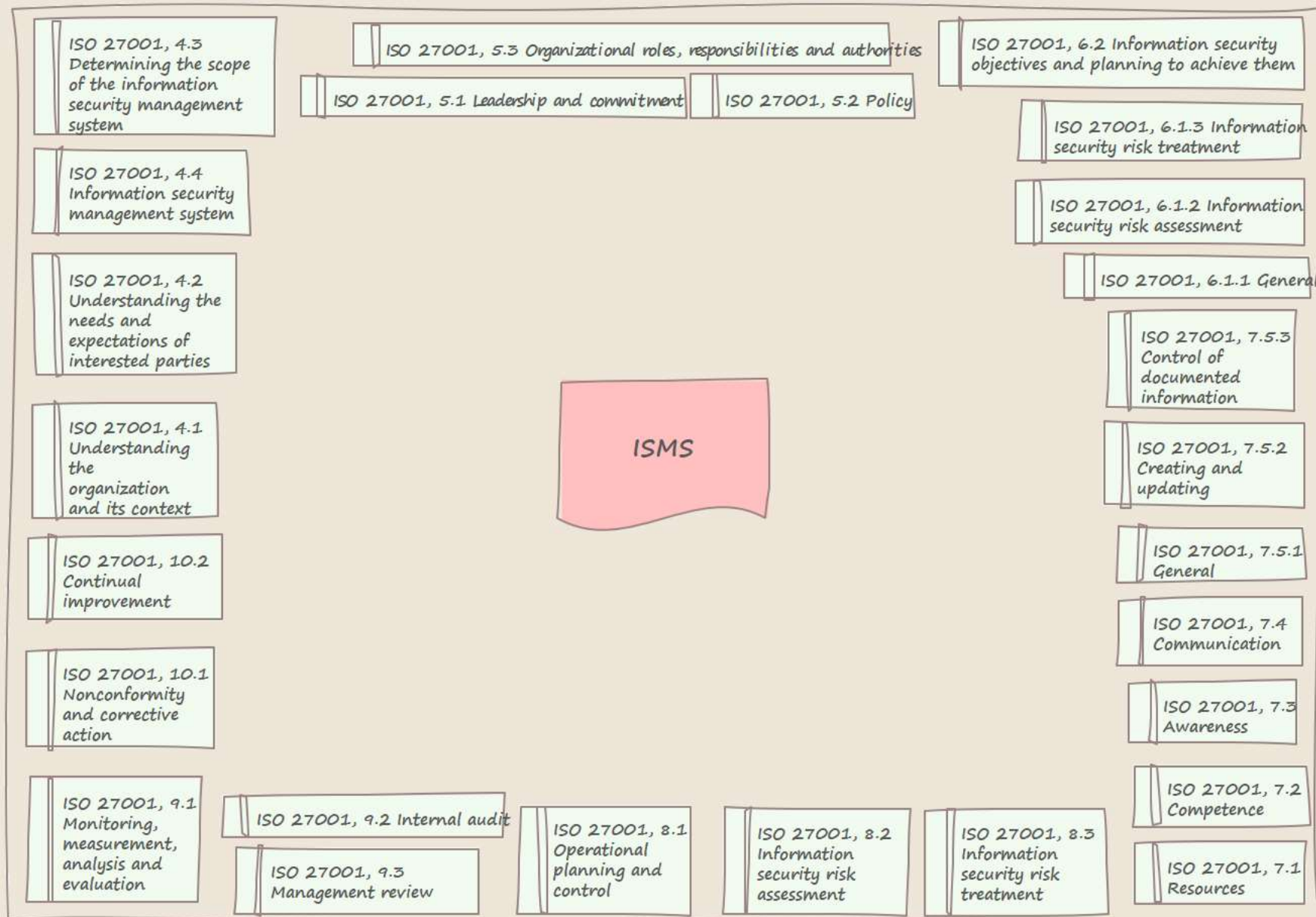
- 45 standarder
- 27000, definitioner
- 27001, krav säkerhetssystemet
- 27002, 114 kontroller
- 27005, hantering av risker

ISO 27001

- Krav mot säkerhetssystemet
- 7 kapitel bondförnuft (23 A4)
- Process: Plan, Do, Check, Act

Nyttan:

- Slipper uppfinna hjulet
- Effektiv väg till säkerhet
- Uppvisad kvalitet (certifiering)



ISO 27001

- Krav mot säkerhetssystemet
- 7 kapitel bondförnuft (23 A4)
- 26 krav

Information **S**ecurity **M**anagement **S**ystem

Ledningssystem för Informations**S**äkerhet

Quality **M**anagement System

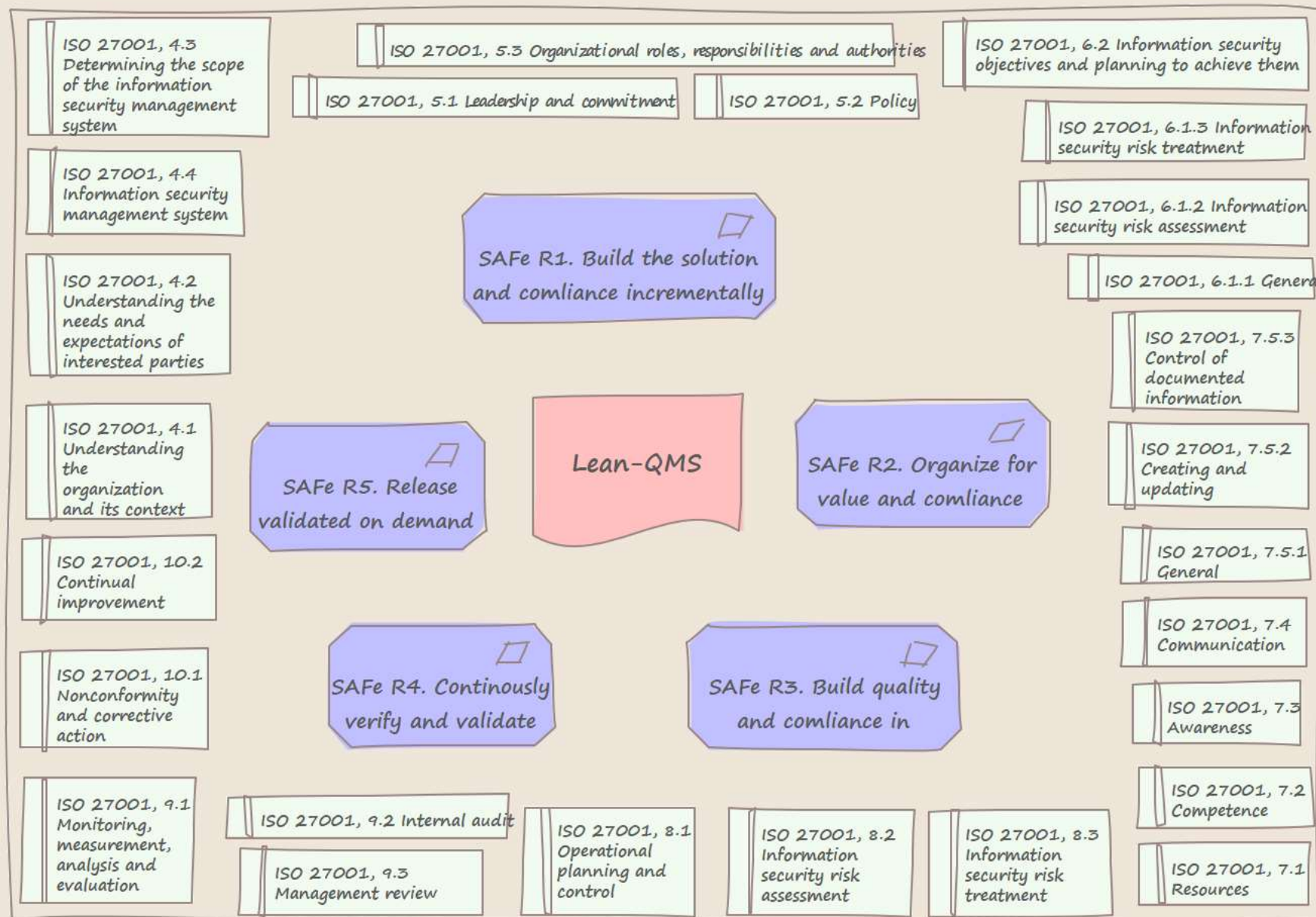
Safe SAFe, två artiklar:

Building in Quality and Compliance

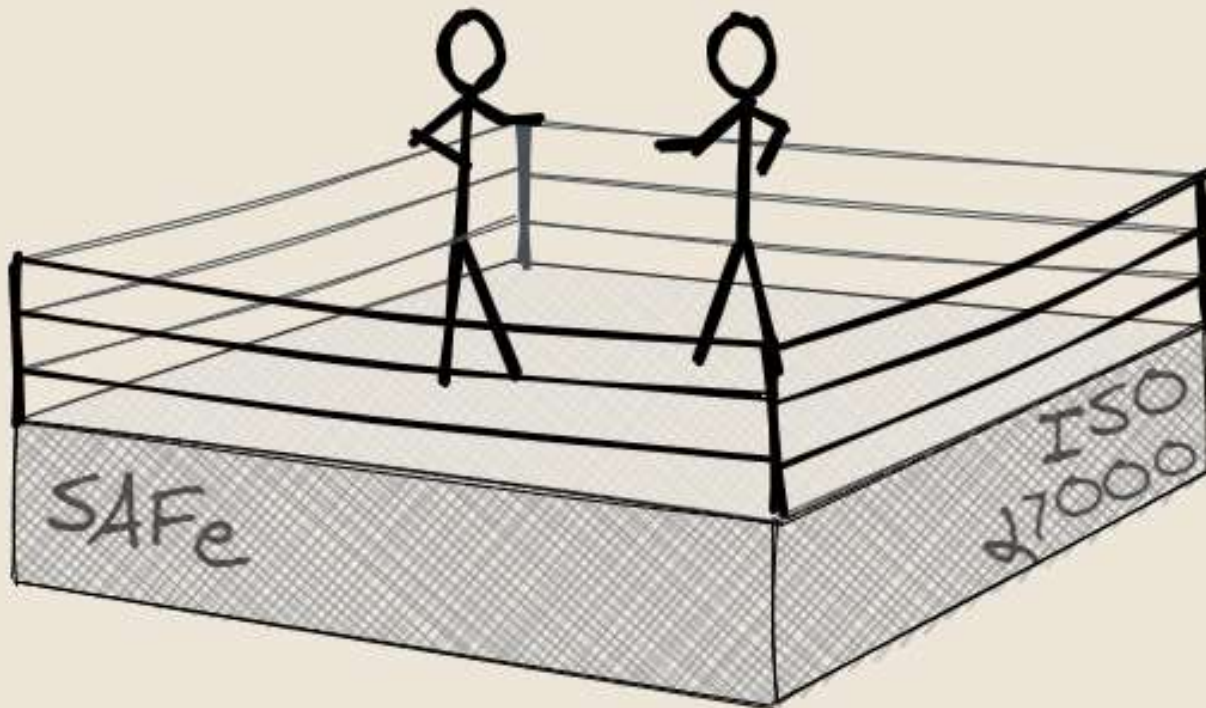
- Kontinuerlig kvalitet och compliance (PDCA)
- Hantera risker tidigt och kontinuerligt
- Integrera kvalitet och compliance i rutinaktiviteter
- DevSecOps

Compliance

- Bygg lösning och compliance inkrementellt (PDCA)
- Inbyggd kvalitet och compliance
- Organisera för värde och compliance
- Lean QMS
- Kontinuerlig, inbyggd V&V

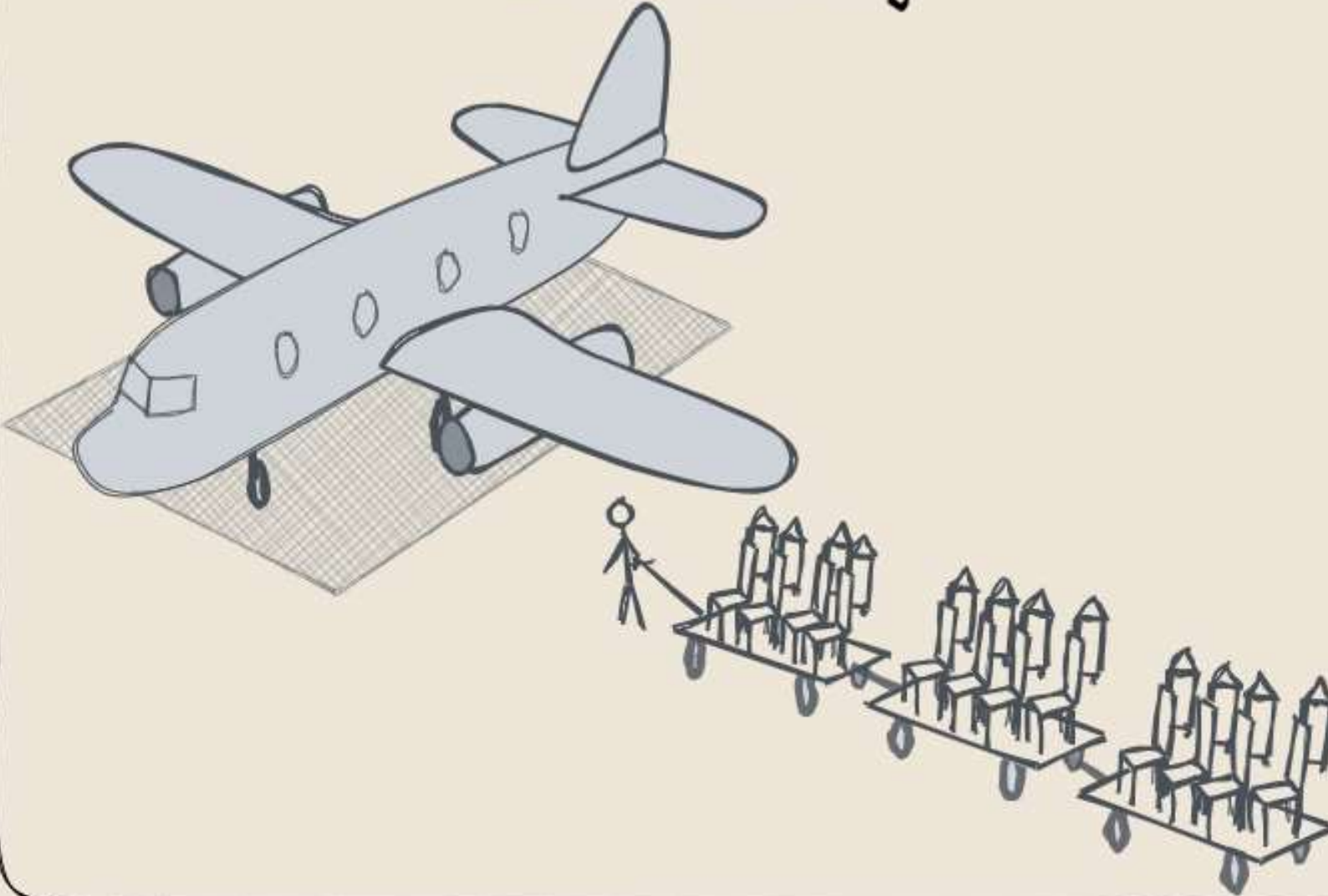


Nu kör vi!



- Kap 4 Sammanhang
- Kap 5 Ledning
- Kap 6 Planering
- Kap 7 Support
- Kap 8 Operativt arbete
- Kap 9 Utvärdering
- Kap 10 Förbättring

Sammanhang



Kap 4, ISO 27001

Organisationens sammanhang

Intressenters behov/förväntningar

Beroenden mellan aktiviteter

=>

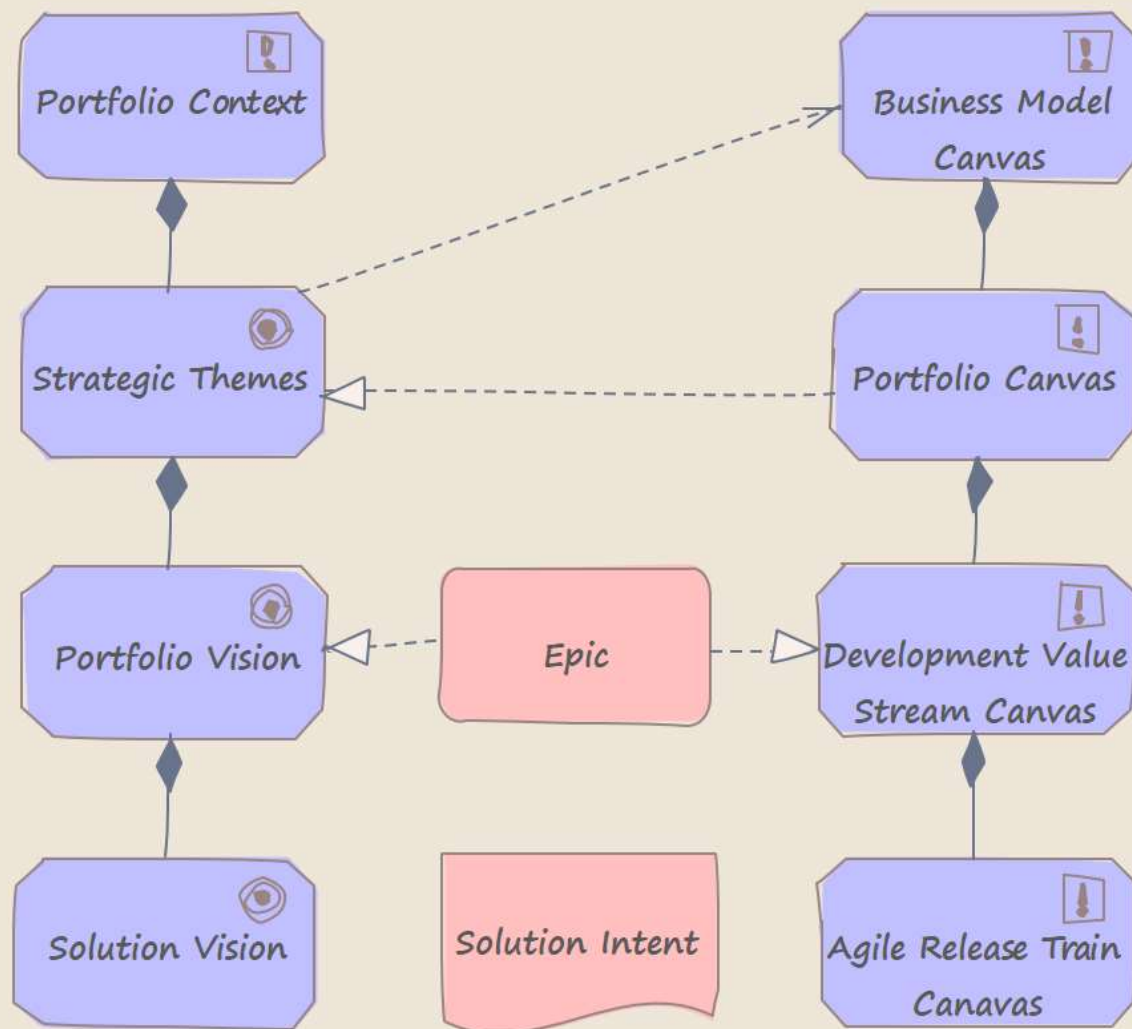
Systemets omfattning

ISO 27001, 4.3
Determining the scope
of the information
security management
system

ISO 27001, 4.4
Information security
management system

ISO 27001, 4.2
Understanding the
needs and
expectations of
interested parties

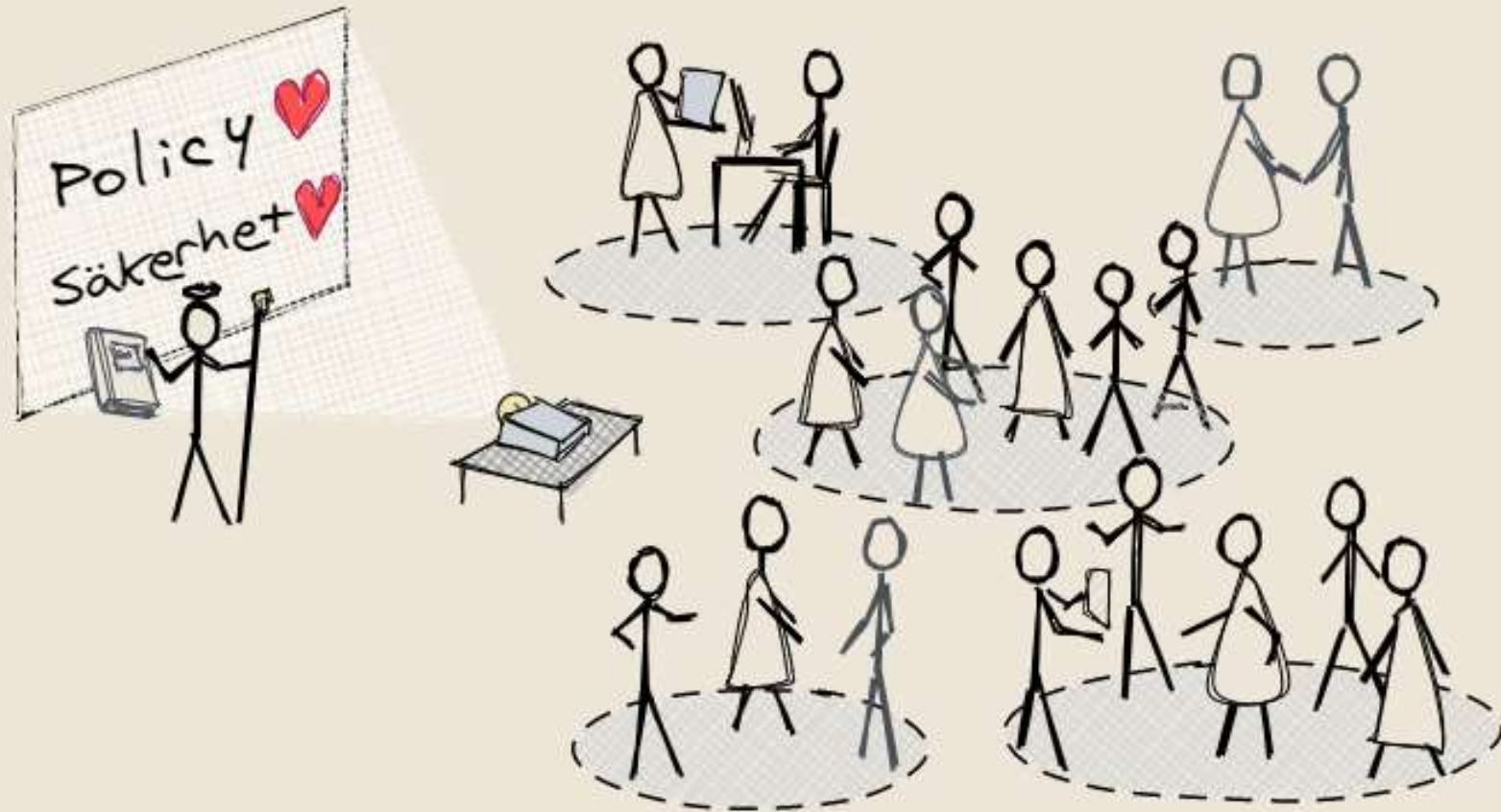
ISO 27001, 4.1
Understanding
the
organization
and its context



Kap 4, Sammanhang, SAFe

- Business Model Canvas - organisationens sammanhang
- Business Model Canvas - Intressenter och dessas behov.
- Operational Value Streams & Development Value Streams - Beroenden / gränssytor
- Solution Intent, Canvas & vision- ISMS omfattning

Ledarskap



Kap 5, ISO 27001

Ledningens engagemang

Säkerhetspolicy

Sätta ansvar & befogenheter

ISO 27001, 5.3 Organizational roles, responsibilities and authorities

ISO 27001, 5.1 Leadership and commitment

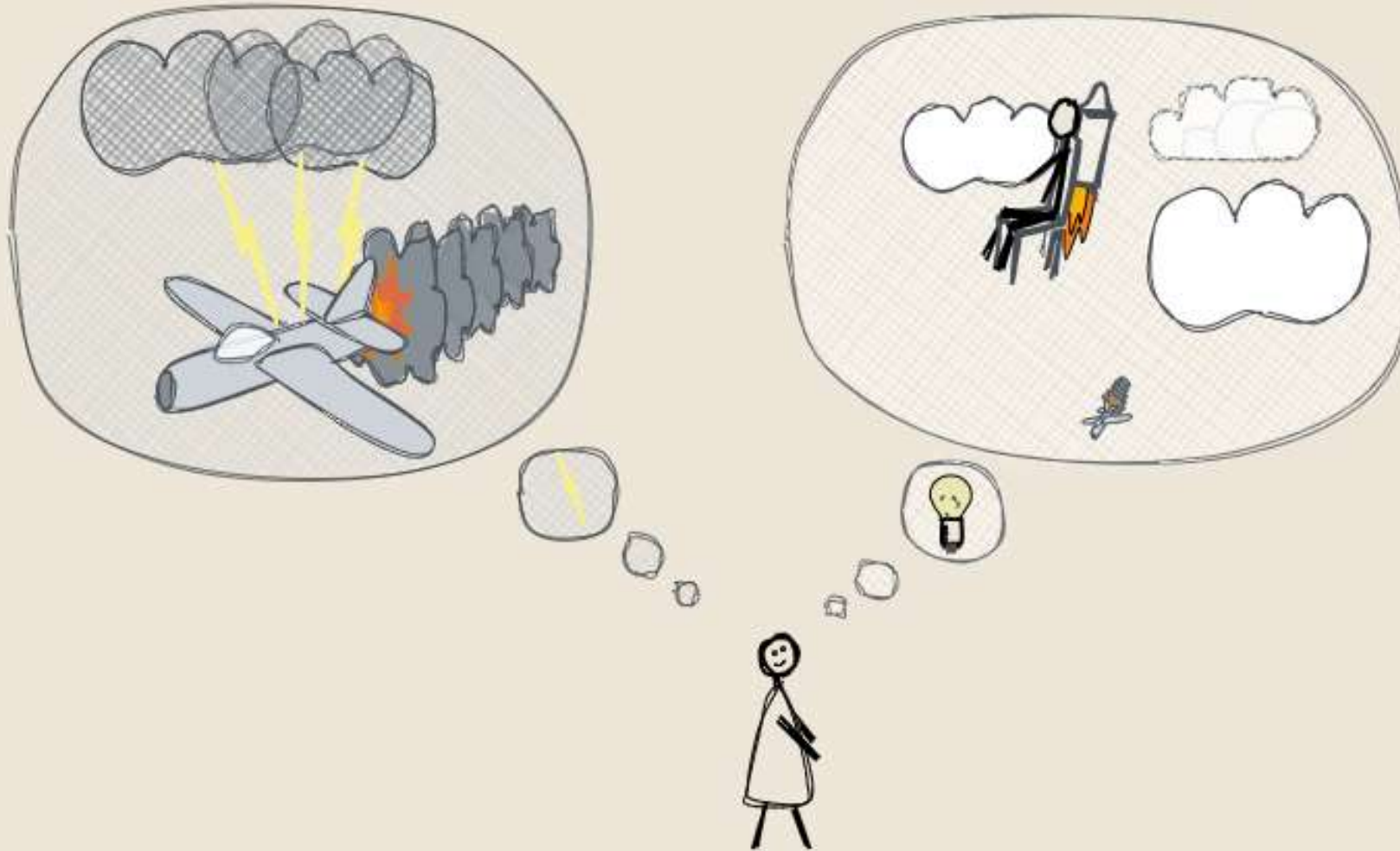
ISO 27001, 5.2 Policy

Lean-QMS

Kap 5, Ledarskap, SAFe

- Lean-Agile Leadership visar ledarskap och engagemang för säkerhet
- Säkerhetspolicy i Lean QMS
- Rollerna i Development Value stream kompletteras med ansvar och befogenheter
- Rollerna i Operational Value stream definieras

Risker och hantering av risker



Kap 6, ISO 27001, Planering

Process för riskanalys

Process för hantering av risker

Säkerhetsmål

Plan för säkerhet

Kap 6, Planering, SAFe

- Processer enligt ISO 27001 kap 6 läggs in i Implementation Roadmap
- Lägg säkerhetskrav i backlog
- Planera i implementation roadmap

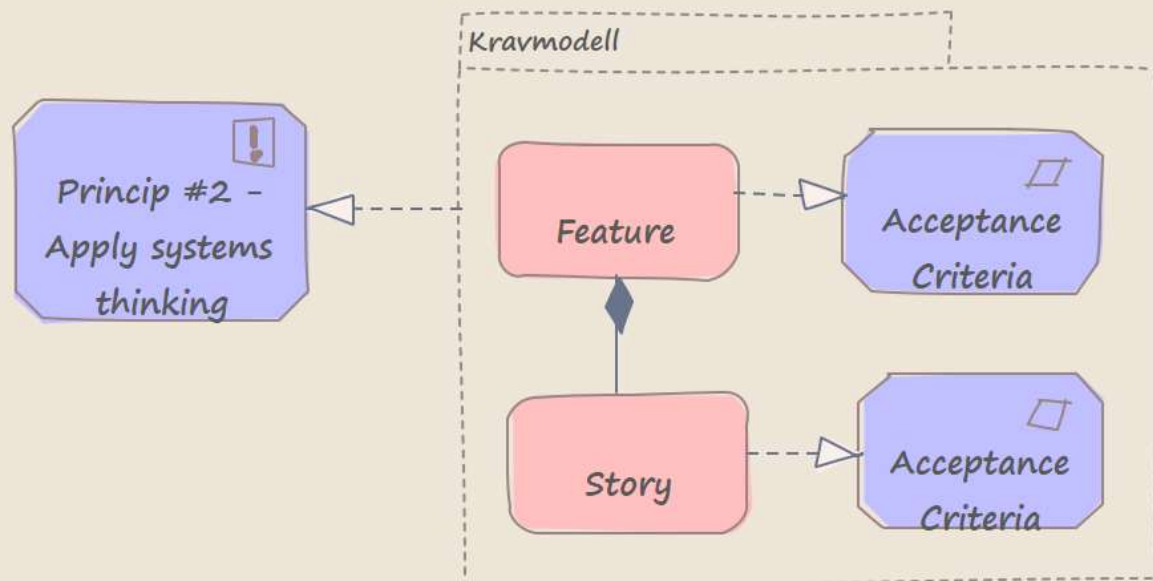
Implementation
Roadmap

ISO 27001, 6.2 Information security
objectives and planning to achieve them

ISO 27001, 6.1.3 Information
security risk treatment

ISO 27001, 6.1.2 Information
security risk assessment

ISO 27001, 6.1.1 General



Resurser



Kap 7, ISO 27001, Support

Nödvändiga resurser

Kompetens: krav & utbildning

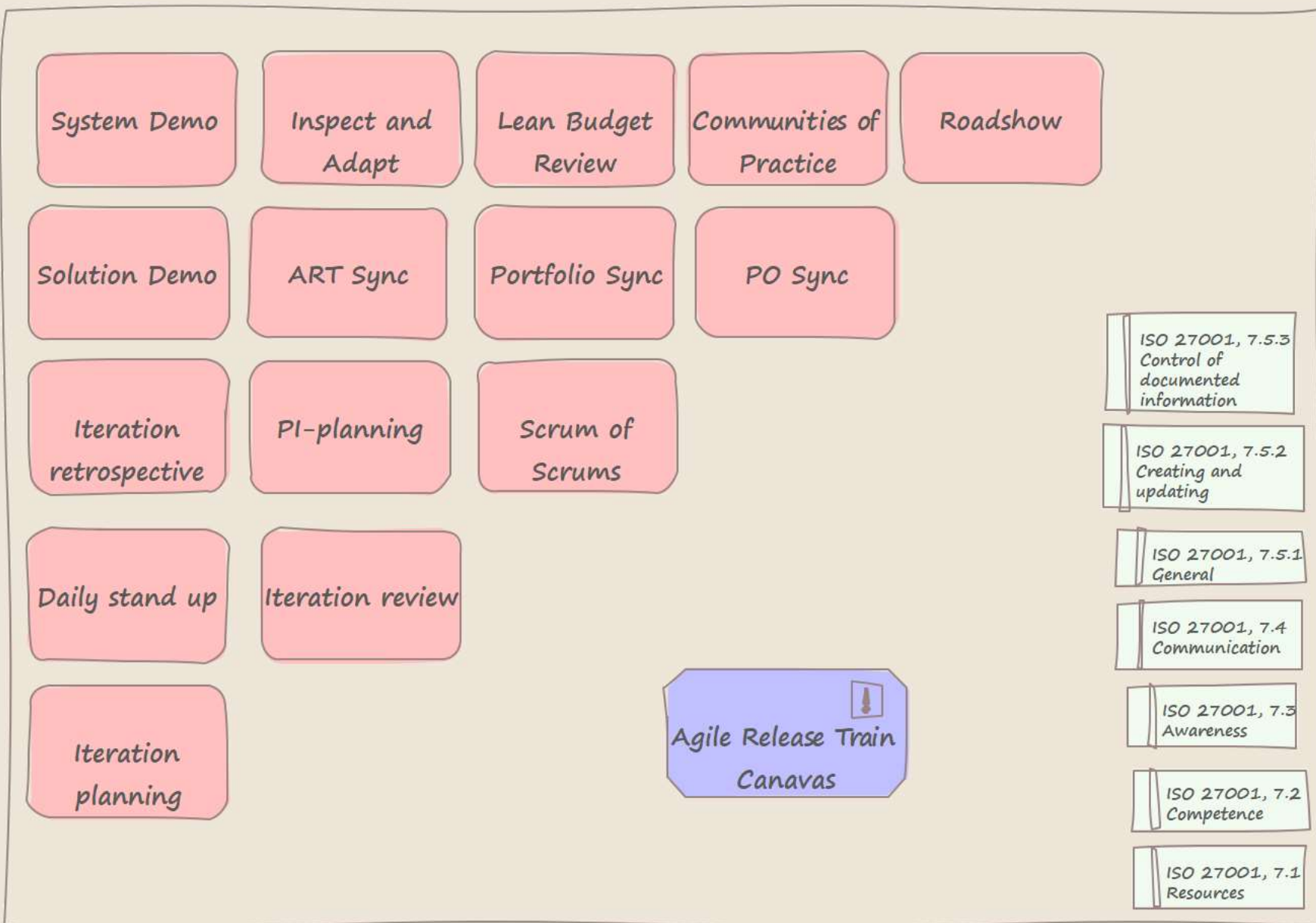
Kommunikation: när, vem, hur

Dokumentation...

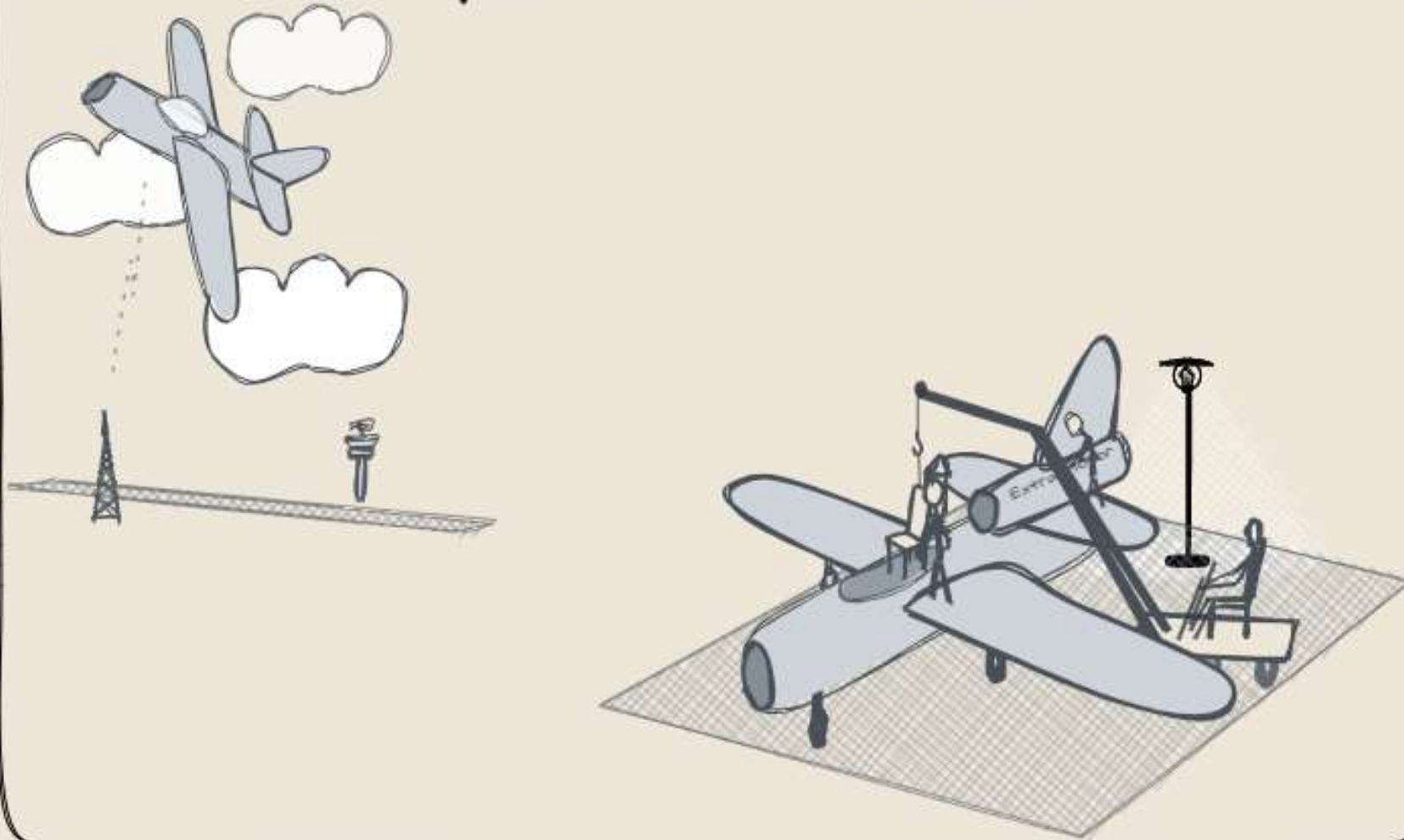


Kap 7, Support, SAFe

- Fastställa vem som behöver kunna vad – Lean QMS
- Planera utbildning
- Planera vad som kommuniceras, när var hur



Operativt arbete



Kap 8, ISO 27001

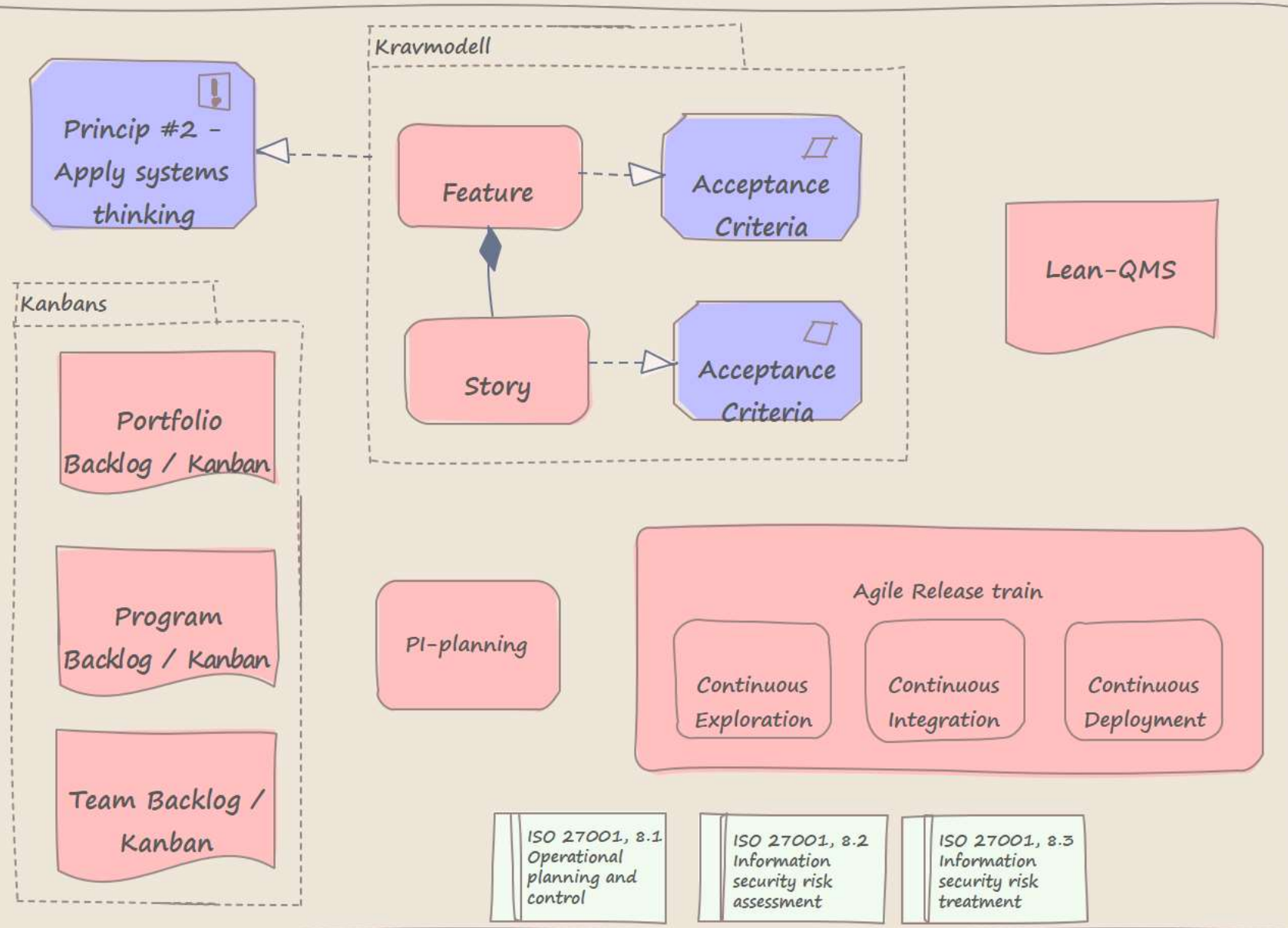
Realisera krav/mål enl kap 6

Hantera ändringar

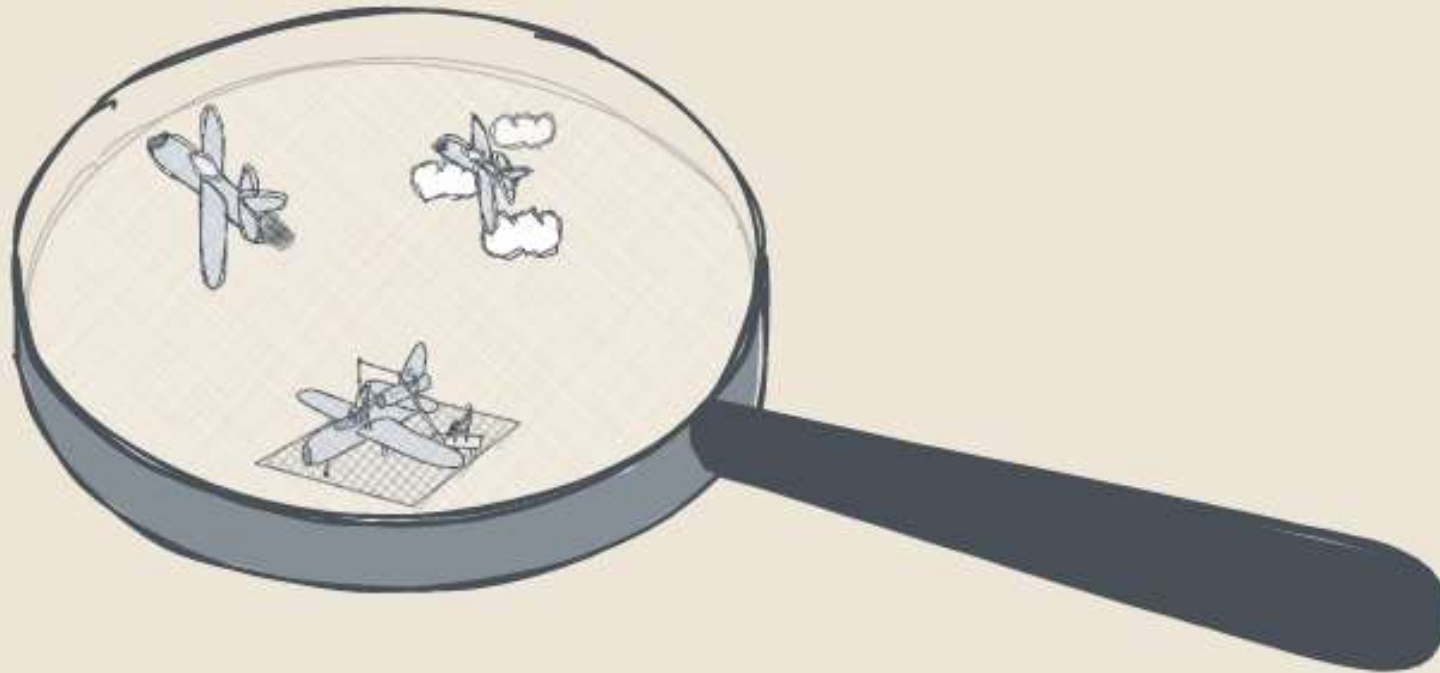
Hantera risker enligt kap 6

Kap 8, Operativt arbete, SAFe

- Implementera säkerhetskraven i backlog
- Lägg kap 6 processer i Continuous Exploration
- Roadmap för säkerhetskraven



Utvärdering



Kap 9, ISO 27001

Utvärdera Effektivitet & resultat

Övervakning & utvärdering

Regelbundna audits

Ledningens granskning

Kap 9, Utvärdering, SAFe

- Var noggrann med KPIer för säkerhetsrelaterade krav
- Inspect and adapt – Planera audits, team granskar andra team, och verksamhet.
- Planera och kör managements reviews för säkerhet
- Förhåll er till Operational value streams

! Principle #5 – Base milestones on objective evaluation of working systems

PI-planning

KPI

Inspect and Adapt

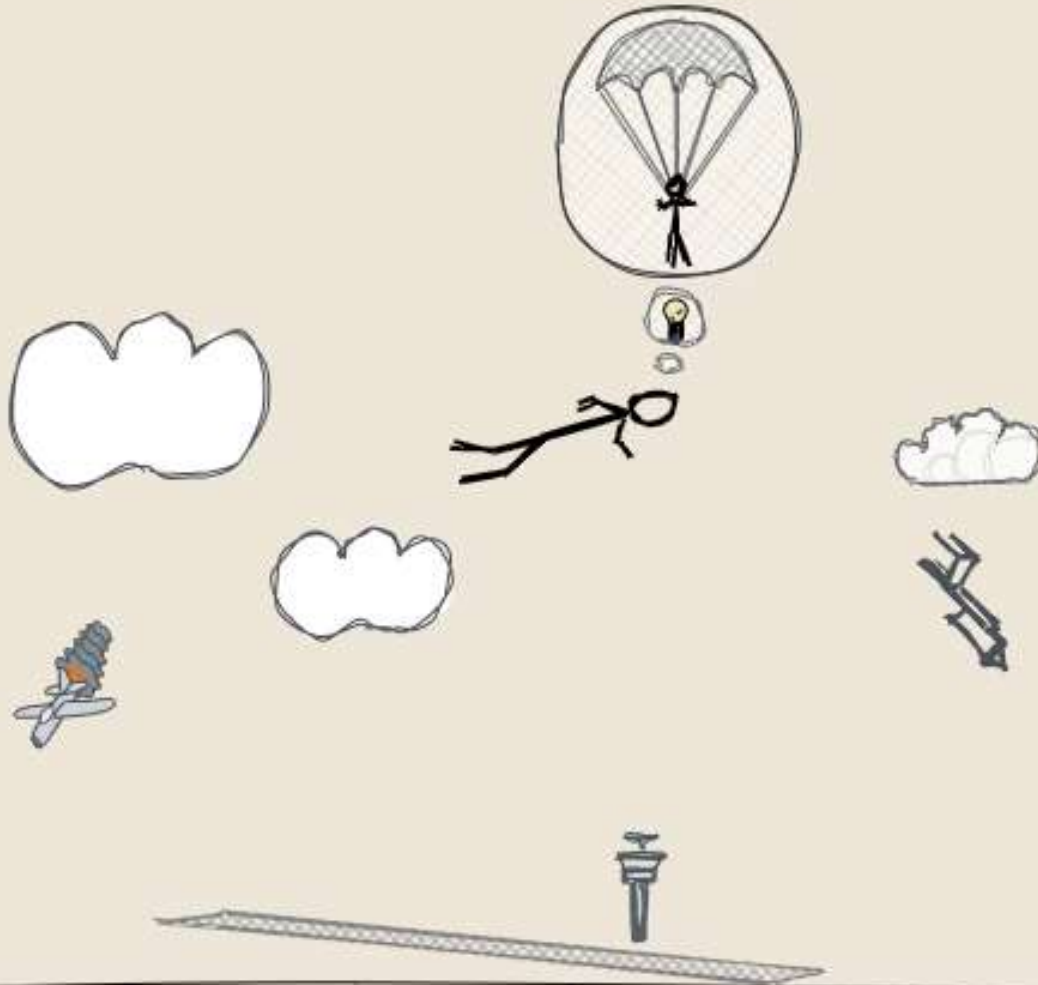
Management Reviews

ISO 27001, 9.1
Monitoring,
measurement,
analysis and
evaluation

ISO 27001, 9.2 Internal audit

ISO 27001, 9.3
Management review

Förbättringar



Kap 10, ISO 27001

Hantera Incidenter

Kontinuerlig förbättring

Kap 10, Förbättringar, SAFe

- Integrera med organisationens incidenthantering
- Skapa processer för att lösa incidenter
- Kör SAFe


Principle #5 – Base milestones on objective evaluation of working systems


Principle #4 – Build incrementally with fast, integrated learning cycles.

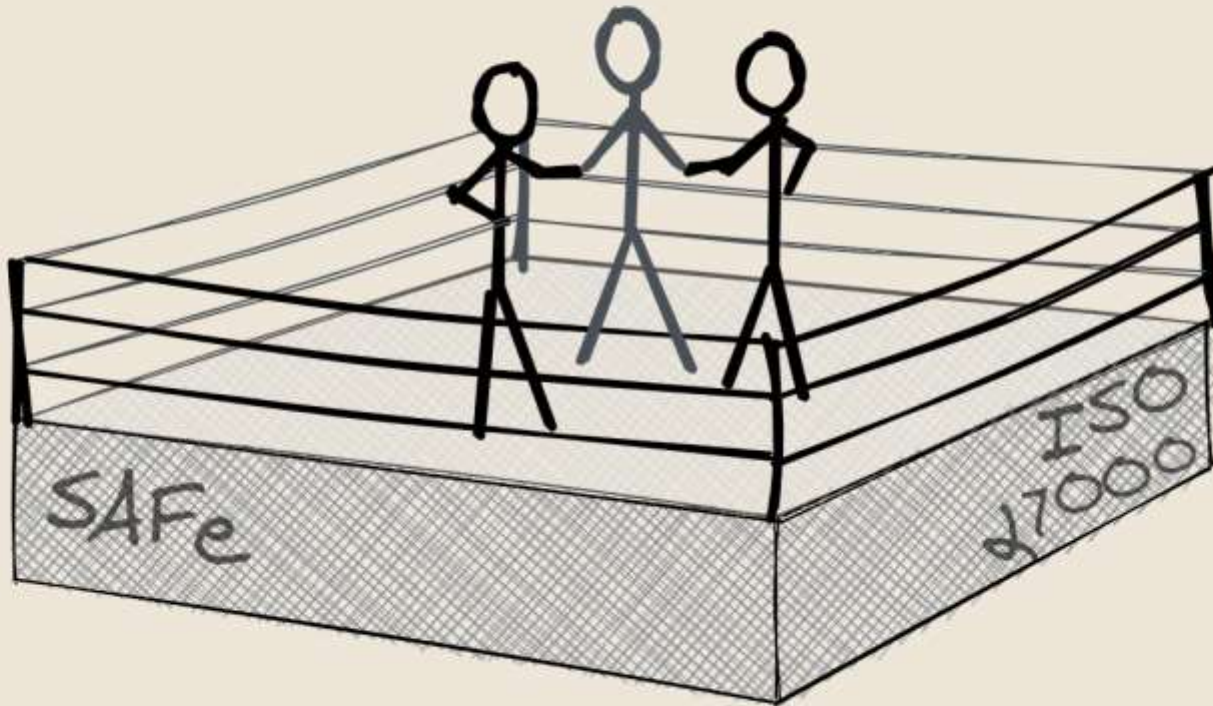
ISO 27001, 10.2
Continual improvement

ISO 27001, 10.1
Nonconformity and corrective action


KPI


Product Management

Hur gick det?



Någon segrare?

Hindrar ISO 27001 SAFe?

Hindrar SAFe ISO27001?

Lärdomar?

Blev det tydligare?

Var inte rädd för snälla spöken!

