Marcell Olsen for Field Talk – November 19th 2026

THE ENTERPRISE CHANGE PARADOX

How Enterprise Architecture and Information Security jointly enable digital transformation and growth

Short introduction



SPEAKER

MARCELL OLSEN

CISO & Head of Enterprise Architecture, Ambu A/S

- **Almost 30 years in technology, including more than 15 in Enterprise Architecture**
- **Energised by turning complex challenges into meaningful change**
- **Experience across DSV, Carlsberg, Pandora and Flying Tiger Copenhagen**
- **Committed to growing talent and sharing what experience has taught me**
- **And still curious!**

The Enterprise Change Paradox

Individually *reasonable decisions* can create collectively *unreasonable change*

Modernise	Protect	Innovate	Respond
Core platforms	Critical operations	AI & connected services	Market opportunities

Fewer surprises to make more ambitious business decisions possible

Shift left on decisions

THE OLD PATTERN

Validate choices already made

- Architecture reviews the solution
- Security assesses risks
- Legal negotiates the contract
- Operations inherits the result

THE BETTER PATTERN

Shape choices while they are open

- Start with outcomes and capabilities.
- Bring disciplines together early
- Surface trade-offs before commitments become hard to reverse.

Create clarity before commitment and make ambitions achievable and trustworthy

Day two on the new job: “We need a new time-registration system”

INITIAL ASK
Replace an ageing time-registration solution

→

BETTER QUESTION
What enterprise capability is missing?

→

CLEARER NEED
Manage projects, portfolios and time allocation

UNDERSTAND THE NEED BEFORE BUYING THE ANSWER

The lesson is to define the right problem at the right time

Make ambition achievable AND trustworthy

EA ASKS

What must we be able to do?

- Business capabilities and outcomes
- Dependencies and sequencing
- Design options and operability
- Future evolution

INFOSEC ASKS

What must customers trust?

- Information and product protection
- Threats and trust boundaries
- Risk decisions and assurance
- Continuity and resilience

A shared capability conversation – far more than a combined reporting line

Roadmaps make cumulative change *visible*



Sequence change to protect today's operations and enable tomorrow's growth.

Different decisions deserve different scrutiny

LIGHT

Guardrails only

- Local, reversible changes
- Known technology pattern
- Low cross-domain impact

STANDARD

Joint review

- Relevant business capabilities
- Security, data or integration impacts
- Documented design choices

STRATEGIC

Enterprise shaping

- Cross-domain transformation
- New business model or trust boundary
- Portfolio and risk-level decisions

Speed and assurance improve when attention is proportional to impact

Ready to sign. But can we *run* what we are buying?

01 **Business need**

02 **Vendor demos**

03 **Preferred bidder**

04 **Contract review**

Then the recovery question lands!!

RECOVERABILITY

DATA EXIT • AI DATA USE
INCIDENT NOTIFICATION

Discover critical requirements while supplier choice and design options are <u>still</u> open

Different expertise changes the choice

Business	EA	InfoSec	Legal	Privacy	Operations
Defines the service outcome	Maps workflows and dependencies	Tests protection and recovery	Shapes viable commitments	Defines permitted data use	Designs how to run and recover

Procurement and Quality help shape supplier choice, evidence and acceptance.

Different disciplines enabling <u>one</u> better-informed choice before commitment

A recovery gap becomes an explicit business choice

Accept the limit	Proceed only if the service need is met and residual risk is authorised.
Change supplier	Test another provider against usable data and workflow recovery.
Change the design	Add a feasible recovery capability, then test ownership, cost and operation.

Compare options before commitment. Mandatory obligations are not optional

Can we transform without disrupting the business?

TODAY

Known estate

- Existing operating patterns
- Legacy controls and debt
- Established responsibilities

TRANSITION

Coexistence

- Temporary interfaces
- Duplicated data and identity
- Moving control boundaries
- Competing change windows

FUTURE

Intended design

- Target capabilities
- Defined control patterns
- Modern operating model

Design and own transition risk to reduce surprises at cutover

Who sees the risk that no single project owns?

PROJECT A

Retires a legacy service

PROJECT B

Changes the identity model

PROJECT C

Migrates critical data

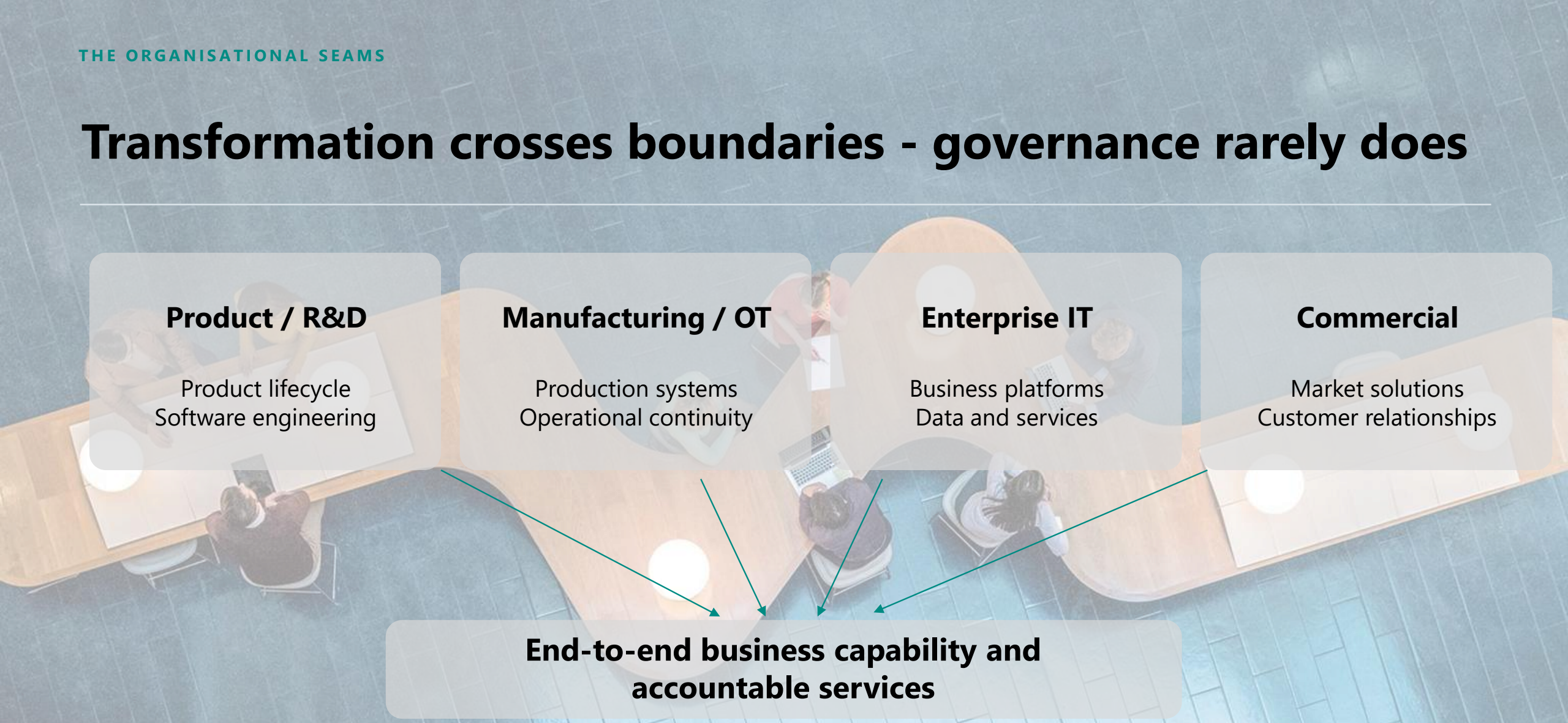
PROJECT D

Introduces new suppliers

COMBINED:
operational dependency + security transition + change capacity

Roadmap intelligence + risk intelligence = a better portfolio conversation.

Transformation crosses boundaries - governance rarely does



Federated expertise - shared decisions - explicit ownership at the boundaries

FROM PHYSICAL PRODUCTS TO TRUSTED DIGITAL HEALTHCARE SOLUTIONS

A future-facing industry scenario

Can we support what we want customers to buy?

PRODUCT-CENTRIC VALUE

Deliver a reliable device

- Quality and safety
- Manufacturing and distribution
- Product lifecycle and field support

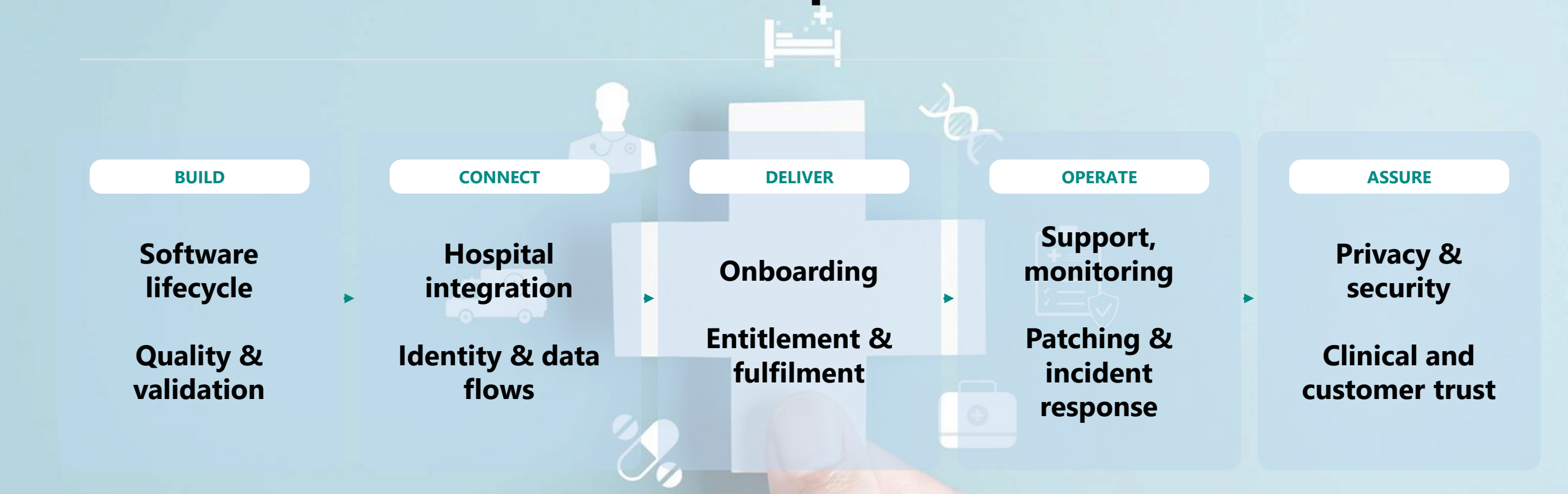
SOLUTION-CENTRIC VALUE

Improve a clinical workflow

- Connected software and services
- Clinical information integration
- Continuous service and assurance
- Potential AI-supported assistance

The commercial offer expands from a product transaction to an enduring service relationship.

Product readiness does not equal business readiness



BUILD	CONNECT	DELIVER	OPERATE	ASSURE
Software lifecycle	Hospital integration	Onboarding	Support, monitoring	Privacy & security
Quality & validation	Identity & data flows	Entitlement & fulfilment	Patching & incident response	Clinical and customer trust

Business-model operability and technology trust must be designed together
Assurance runs through every stage

Information Security is part of the growth engine

PROTECT

Existing value

Protect operations, information and product integrity. Keep the current business dependable.

TRANSFORM

Change responsibly

Manage emerging threats, trust boundaries, transitional exposure and risk decisions.

GROW

Earn external confidence

Provide **repeatable** security and resilience evidence that supports customer decisions and deployment.

Trust makes an ambitious offer credible and operability makes it deliverable

Digital trust must survive the sale

SECURITY & INTEGRITY

Protect devices, patient information and critical functions

PRIVACY & DATA GOVERNANCE

Lawful use, transparency, appropriate controls

CLINICAL & SERVICE RELIABILITY

Evidence, safety, operational performance

LIFECYCLE ASSURANCE

Vulnerabilities, updates, incidents, resilience

Trust begins with a promise and grows through consistent evidence

Five changes to take into your next decision

1. Ask “what problem do we need to solve?” before “which platform?”
2. Shape commitments with Legal, Privacy and Operations **early**
3. Map cumulative change and transitional exposure
4. **Design what customers must trust and teams must operate**
5. Measure decision quality over time

Start with <u>one</u> consequential decision and <u>one</u> colleague from another discipline.

AUDIENCE TAKEAWAY

A collaboration model you can use tomorrow

DEFINE

Business outcomes
Capabilities
Portfolio

→

DECIDE

Joint requirements
Options & risk
Sourcing

→

TRANSFORM

Transition states
Dependencies
Exceptions

→

OPERATE

Service ownership
Assurance
Feedback

Common decision points · Named owners · Shared evidence · Proportionate review

Assurance runs through *every* stage

Questions worth taking back to your organisation

DECISIONS

Who enters early?

Do EA, InfoSec, Legal and IT Operations influence business requirements *before* a supplier is preferred?

CHANGE

Who sees the whole?

Can anyone explain cumulative transition risk across initiatives and organisational boundaries?

TRUST

Who can prove it?

Can we demonstrate the assurance and operating capability behind the digital promises we make?