GOTO **COPENHAGEN**

Craft software with confidence in 2026

CONTINUOUS DELIVERY & COMPLIANCE

Compliant, Not Slow

Shipping Every Day in a Highly Regulated Environment

Anders Sveen

GOTO COPENHAGEN 2026

PRINSIPALIS

01 / 05

Continuous delivery

WHAT I CARE ABOUT

Build step by step. Check against real feedback from production.



“Our desire to have predictable features and predictable roadmap are entirely at odds with the humility needed to actually innovate and just say ‘we don’t know yet.’”

— Marty Cagan

Photo: Apetitu, CC BY 2.0, Wikimedia Commons

WHAT I CARE ABOUT

Own what you ship. Care about the people using it.

Stable teams. Real ownership. Learn from users.

You ship it. You own it. You maintain it.

IN PRACTICE: CONTINUOUS DELIVERY, IN SMALL PIECES

2–10

DEPLOYMENTS A DAY

Sometimes more.

THE RESEARCH: ACCELERATE

Deploying that often sounds risky.

The teams that deploy most often also fail least, and recover fastest.

Speed and stability are not a trade-off.

DOING IT RESPONSIBLY

Feature toggles

deployed is not the same as released

Smaller changes

less to go wrong, easier to review

Metrics and telemetry

know quickly when something is off

Risk evaluation

judgement per change, secure and isolated, built into the process

MOVING FAST THROUGH ENVIRONMENTS

Test in dev, even when the feature isn't live in prod.

But be sure it is not accessible, or enabled, in prod.

That takes a different mindset than “don’t merge until it’s done”. The safety moves from the branch to the toggle.

Anders Sveen

20+ years building software

Agile, DevOps and Continuous Delivery

Prinsipalis

Previously: Porterbuddy, ZTL Payments, Banking and Finance Consulting

Today: consulting at BankID, my main customer, and others

BankID did the certification. The views are mine.



Oslo, from Ekeberg — Dimitri Neyt, public domain, Wikimedia Commons

02 / 05

BankID & regulations

The domain, and what certification asks of it

bankID

THE DOMAIN

Digital identity. Proving who someone is, online.

BankID since 2004: a code device, then an app, now biometrics. About a billion logins a year.

A trust service under eIDAS. Certified against ETSI standards.

bankID

4.6M

NORWEGIANS HAVE BANKID

Banking · Tax returns · Welfare · **Health records**

Essentially the only widely used eID trusted with your health data.

A lot of different kinds of users.





“Analogue child, without BankID / MitID”



HEAVILY REGULATED

Regulated is too often slow.

Nobody sets out to slow you down. It is just hard to dig out what is actually required.

Photo: Oulu county archive, 1933 — Finnish Heritage Agency, CC BY 4.0

WHAT AN AUDITOR LOOKS FOR

Know what you have. Know how you do things. Document that. Verify you do what you say.

Do you have processes?
Do you follow them?
Do you have proof?
Do you manage your risks?

Protect.
Document.
Verify.

03 / 05

Getting certified

A NEW PRODUCT, AND NOT A ONE-OFF

Identity proofing was built first. Certified after.

More systems will need certifying.

GETTING CERTIFIED

Choose an auditor

Map out the requirements

Get certified

Not that easy.
It is a process.

THE AUDITOR

Auditors are not scary.

Working together to get everything according to spec is the goal.

04 / 05

Approach

Protect, and prove it



Photo: desilia, CC0, Wikimedia Commons

WHAT MAKES THAT POSSIBLE

Trusted roles.
The right people have the right training, access and knowledge at the right time.

Nobody has standing access. You ask, someone else approves, and it expires.

MAKE THE HARD EASY

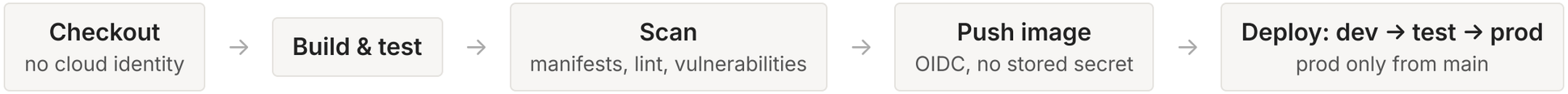
Highly Secure is usually the scary tier.
For us it is where we deploy new features, every day.

"If it hurts, do it more frequently, and bring the pain forward." — Jez Humble

TWO MAIN CONCERNS

No one, however trusted, can do harm alone.
If anyone messes up, known or unknown, it gets noticed.

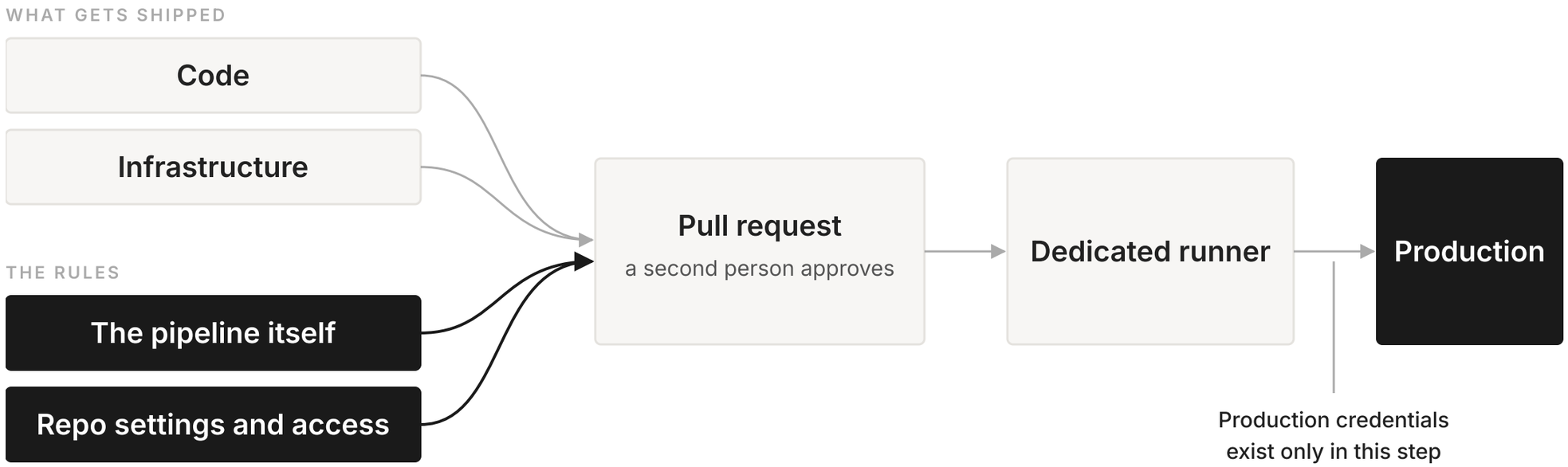
LEAST PRIVILEGE, FOR THE PIPELINE TOO



A different, scoped identity for every environment. No identity at all until it's actually needed.

Only this one repo can use those credentials. Who has access to the repo is the start of the chain.

WHY WHAT IS DEPLOYED CAN BE TRUSTED



The rules change the same way the code does.

EVIDENCE, COLLECTED AUTOMATICALLY

Every production deploy registers itself as a change record in Jira.

TOOLS

Docker Terraform Git Trivy

Kubernetes

GitHub Dependabot

Signed commits Azure



NETWORKS, OR ZONES

Older standards talk about networks.

Newer ones talk about zones.

But people still read them in the language of networks.
Tradition is hard to get rid of.

Photo: public domain, Wikimedia Commons

WHAT A ZONE IS

Common control. Common security level.

Software-defined networking is accepted. In the cloud, it is the standard.

Look past the wording.
Understand the concern.

DID THE AUDITOR DEMAND IT?

The certification sets the floor. Where the risk assessment says more, do more.

HOW MUCH RISK IS ACCEPTABLE?

The standard doesn’t say.

Decide. Be proportionate. Write it down. Someone accountable signs for what is left.

HOW DETAILED?

Define what you do. Know that you do it.

You choose the level.

05 / 05

Where it’s going

What can be better, and where compliance is heading

WHAT YOU CAN AUTOMATE

The old way: read the docs, spot-check production.

Automate evidence collection

Detect drift programmatically

Do it continuously

WHERE THIS SHOULD GO: CONTINUOUSLY

Slow loop: are these still the right rules?

Fast loop: does production still match them?

Automatic drift detection. Partly there: drift would be found, but it leans on people noticing. It should be the system saying so.

Git, diffs and source control, all the way down.

AND WITH AI

AI doesn't replace good practices.

It amplifies them.

Small steps, fast feedback and guardrails let agents move fast. Without them, things just go wrong faster.

CONTINUOUS COMPLIANCE

An audit is a snapshot, read once a year.

If the answer is true every minute, there is a live one to read instead.

WHAT IT WILL NEVER BE

Not everything will be documented. The important parts have to be.

The rest rests on trust in the process.

WHERE THIS IS GOING

Continuous delivery.
And continuous compliance.

Look past the wording. Understand the concern.

RATE MY TALK

GET REWARDED

THANK YOU

Compliant, Not Slow

Anders Sveen

@anderssv · blog.f12.no · linkedin.com/in/anderssv

LINKEDIN

PRINSIPALIS.NO

PRINSIPALIS