Why governance matters: the key to reducing risk without slowing down

Sarah Wells

sarahwells.dev

Why governance matters: the key to reducing risk without slowing down

Sarah Wells

sarahwells.dev

“Governance” has an image problem

FTSE 100 +0.77% | S&P 500 +0.59% | Euro/Dollar −0.01% | Pound/Dollar −0.03% | Brent Crude Oil −0.54% | 10 Year US Gov +0.24% | Visit Markets Data

FINANCIAL TIMES

Subscribe | Sign In

HOME WORLD UK COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

Jaguar Land Rover Ltd

‘Moral hazard’ warning after £1.5bn government loan guarantee for JLR

Carmaker receives official backing after cyber attack that has halted production

3 HOURS AGO

How does cyber insurance work – and why don’t all companies have it?

Keir Starmer

Starmer urges Labour to unite for ‘fight of our lives’ ahead of conference

Editor's picks

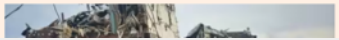
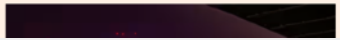
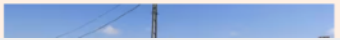
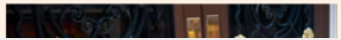
“There is no shame in sleeping late

Pilita Clark

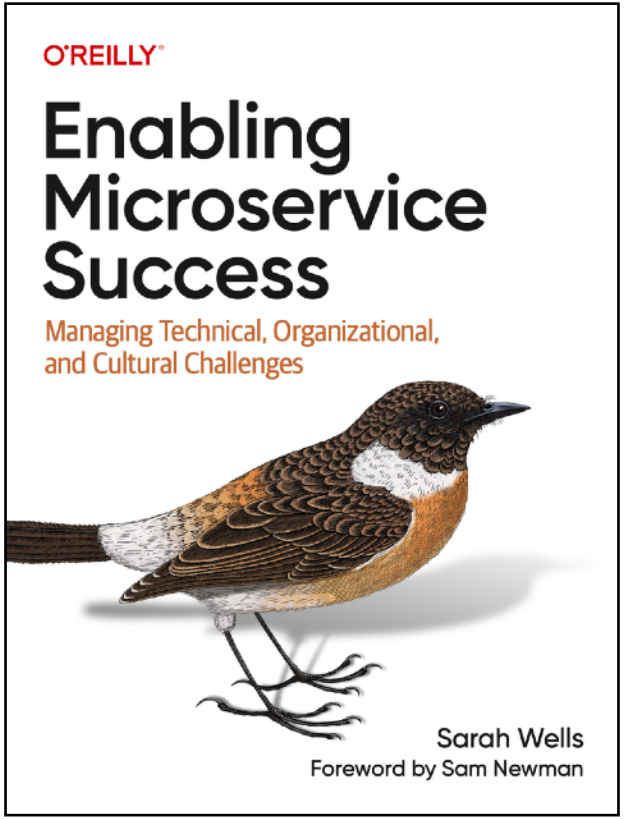
“Why CEOs are right to stick close to Trump

Tevi Troy

TOP STORIES

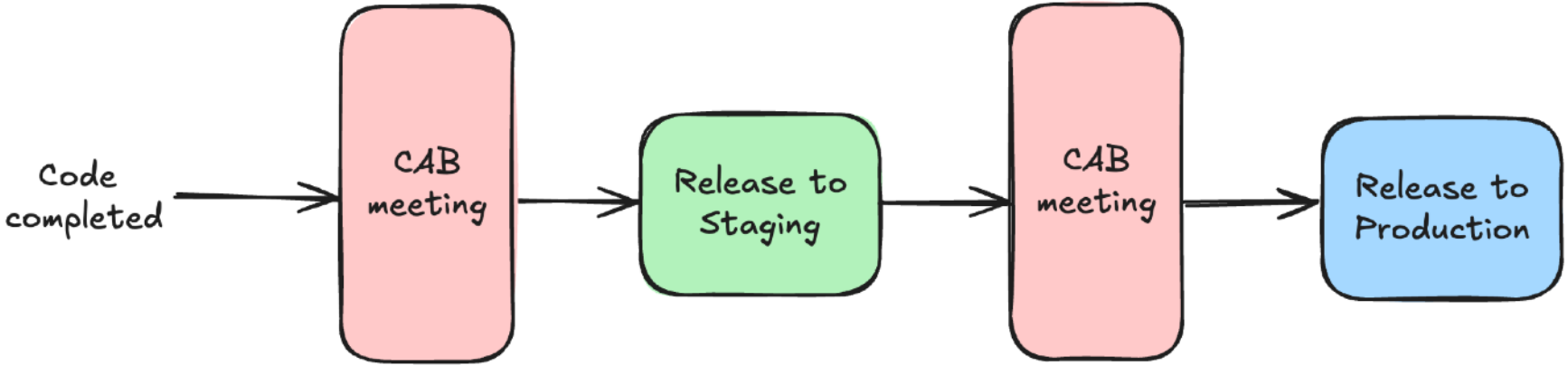
sarahwells.dev

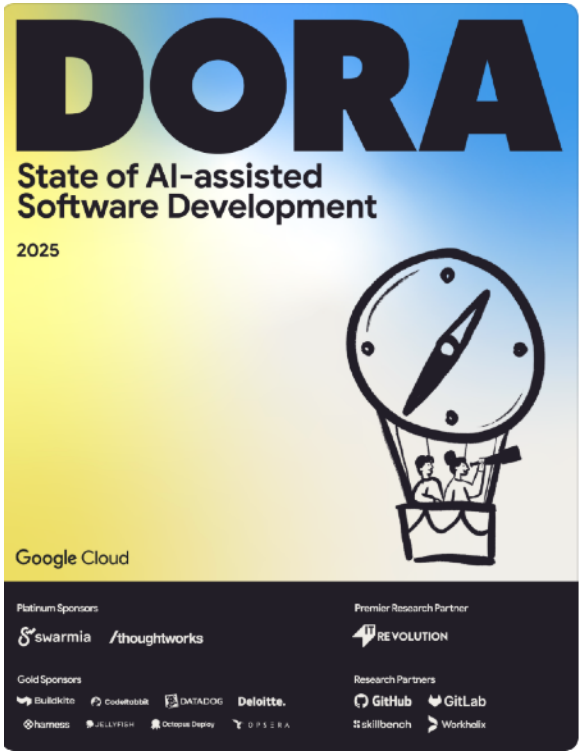


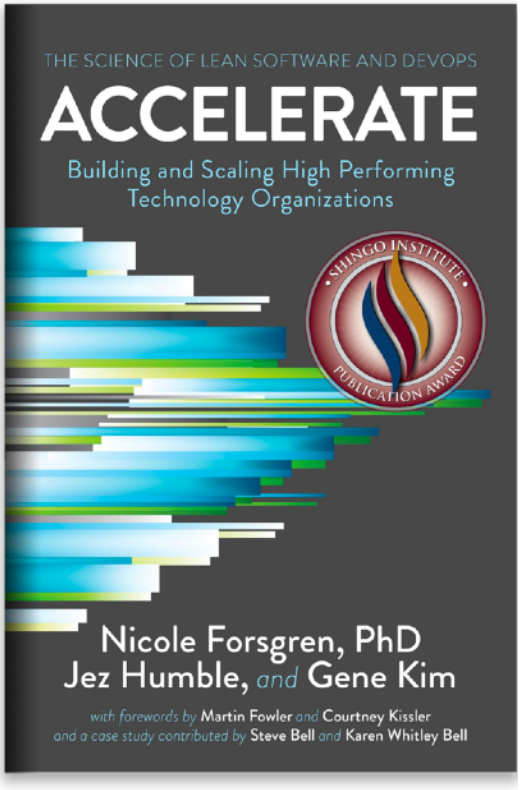

sarahwells.dev

Change Advisory Boards

“a group that reviews, evaluates, and approves or rejects proposed changes”


Code completed
CAB meeting
Release to Staging
CAB meeting
Release to Production


DORA
State of AI-assisted Software Development
2025
Google Cloud
Platinum Sponsors
swarmia
thoughtworks
Premier Research Partner
REVOLUTION
Gold Sponsors
Buildkite
CodeRabbit
DATADOG
Deloitte.
harness
JELLYFISH
Octopus Deploy
OPSERA
Research Partners
GitHub
GitLab
skillbench
Workhelix

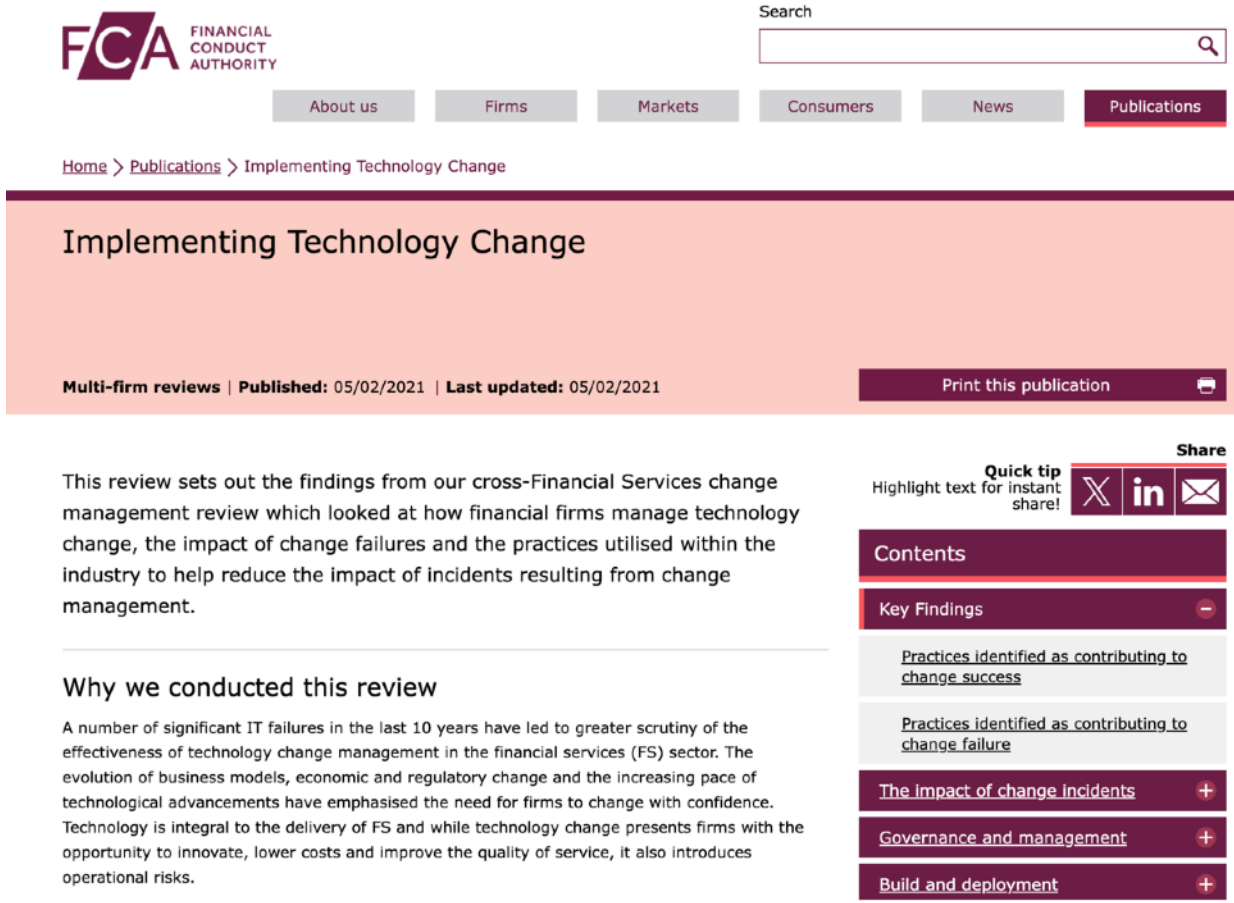

THE SCIENCE OF LEAN SOFTWARE AND DEVOPS
ACCELERATE
Building and Scaling High Performing Technology Organizations
SHINGO INSTITUTE
PUBLICATION AWARD
Nicole Forsgren, PhD
Jez Humble, and Gene Kim
with forewords by Martin Fowler and Courtney Kissler
and a case study contributed by Steve Bell and Karen Whitley Bell

“approval by an external body simply doesn’t work to increase the stability of production systems”

Accelerate, Forsgren et al, 2018

“However, it certainly slows things down.”

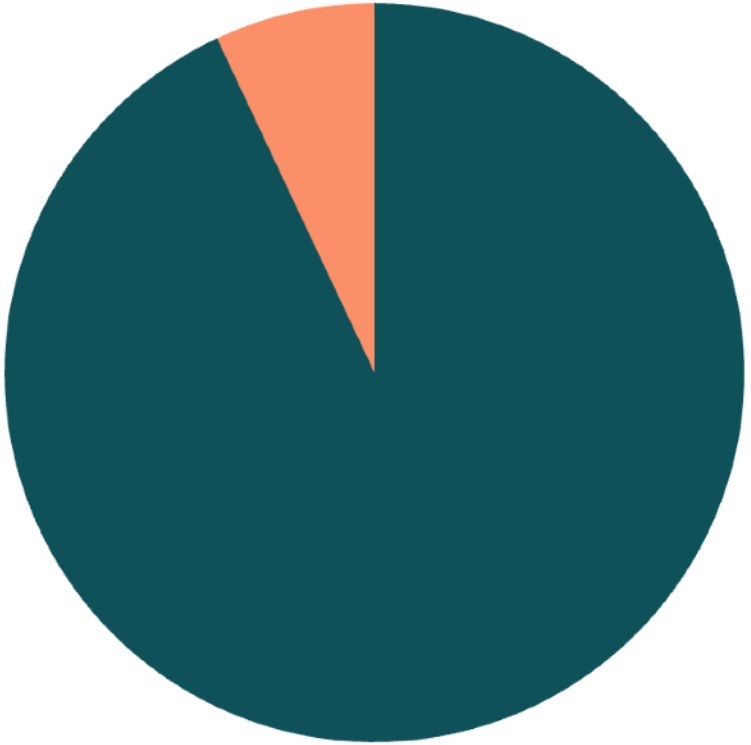
Accelerate, Forsgren et al, 2018



https://www.fca.org.uk/publications/multi-firm-reviews/implementing-technology-change

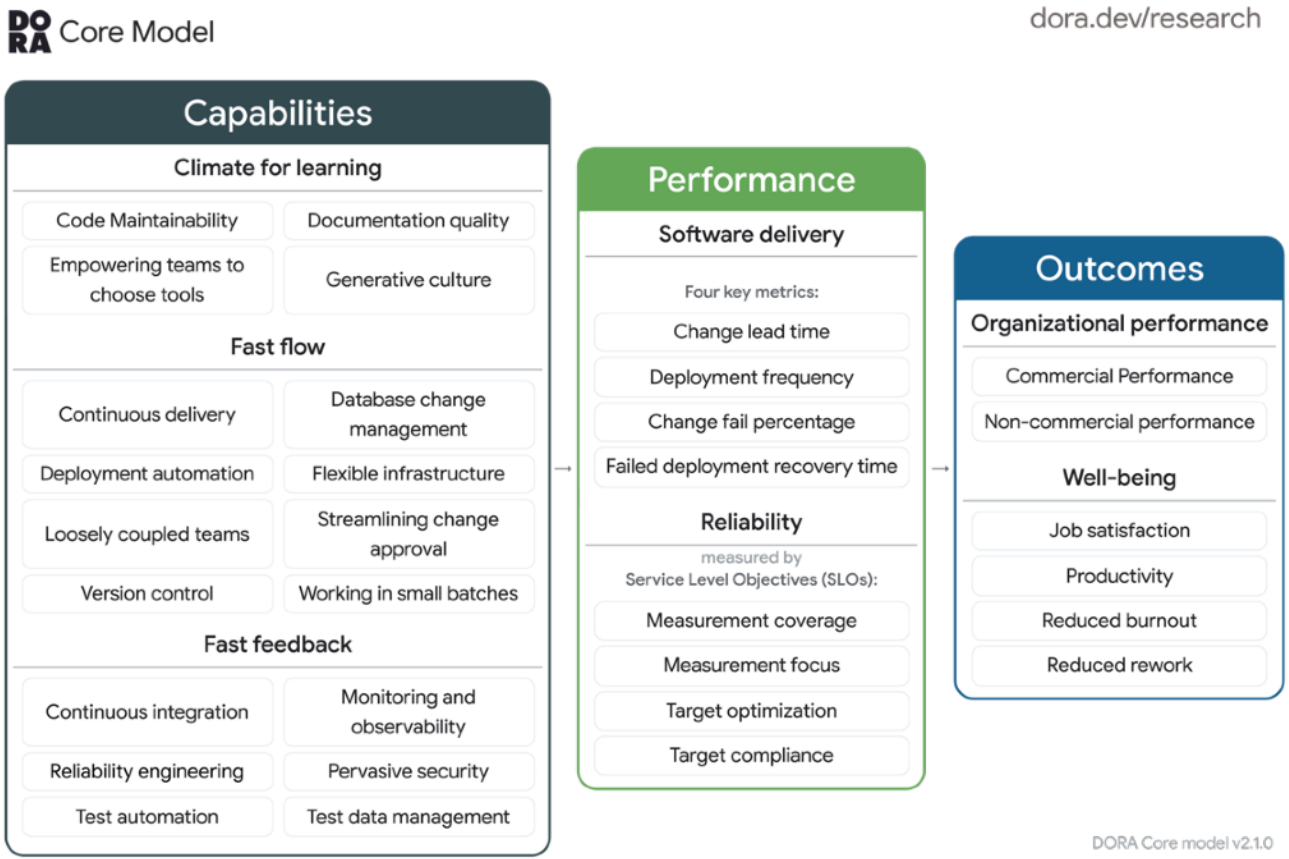
sarahwells.dev

CABs approved 93% of major changes



“This raises questions over the effectiveness of CABs as an assurance mechanism”

What’s my point?



DORA Core, https://dora.dev/research

sarahwells.dev

Effective teams are autonomous - which requires loose coupling

CAB groups don’t have the context

Catch issues through good observability

CABs were just one example

Making the case for governance

Salesloft Drift breach, August 2025

sarahwells.dev

Informational Message

INFORMATIONAL MESSAGE DETAILS ID# 20000217 | ONGOING

Security Advisory: Unusual Activity in a Third Party Connected App

We want to inform our customers about a recent security incident involving the Drift app, published by Salesloft, that was installed by individual customers. Salesforce security teams detected unusual activity that may have resulted in unauthorized access to a small number of customers' orgs data via the app's connection to Salesforce.

It is important to note that this issue did not stem from a vulnerability within the core Salesforce platform, but rather from a compromise of the app's connection.

Upon detecting the activity, Salesloft, in collaboration with Salesforce, invalidated active Access and Refresh Tokens, and removed Drift from AppExchange. We then notified affected customers.

We're continuing to work with Salesloft as part of our investigation and provide updates as appropriate, including notifying and supporting affected customers with remediation. If you need support, please reach out through Salesforce Help: https://help.salesforce.com/s.

https://status.salesforce.com/generalmessages/20000217

sarahwells.dev

Mandiant Incident Response

Investigate, contain, and remediate security incidents.

Learn more

Recommendations

Given GTIG's observations of data exfiltration associated with the campaign, organizations using Salesloft Drift to integrate with third-party platforms (including but not limited to Salesforce) should consider their data compromised and are urged to take immediate remediation steps.

Impacted organizations should search for sensitive information and secrets contained within the integrated platforms and take appropriate action, such as revoking API keys, rotating credentials, and performing further investigation to determine if the secrets were abused by the threat actor.

https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

sarahwells.dev

The impact of the Salesloft Drift breach on Cloudflare and our customers

2025-09-02

 Sourov Zaman  Craig Strubhart  Grant Bourzikas

12 min read

This post is also available in 简体中文, Français, Deutsch, 日本語, 한국어, Português, Español (Latinoamérica), العربية and 繁體中文.

https://blog.cloudflare.com/response-to-salesloft-drift-incident/

 sarahwells.dev

Responding to this breach

Lots of AI FOMO

An incident involving many teams

Do you understand what data you have where?

Governance at Drift

Mandiant's investigation has determined the threat actor took the following actions:

- In March through June 2025, the threat actor accessed the Salesloft GitHub account. With this access, the threat actor was able to download content from multiple repositories, add a guest user and establish workflows.

- The threat actor then accessed Drift's AWS environment and obtained OAuth tokens for Drift customers' technology integrations.

https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

sarahwells.dev

Mandiant's investigation has determined the threat actor took the following actions:

- In March through June 2025, the threat actor accessed the Salesloft GitHub account. With this access, the threat actor was able to download content from multiple repositories, add a guest user and establish workflows.

https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

sarahwells.dev

Mandiant's investigation has determined the threat actor took the following actions:

- In March through June 2025, the threat actor accessed the Salesloft GitHub account. With this access, the threat actor was able to download content from multiple repositories, add a guest user and establish workflows.

Furthermore, we are implementing new multi-factor authentication processes and further refining limitations to the application environment. These measures are complemented by an ongoing analysis of available logs and configuration settings, as well as the remediation of secrets within the environment and GitHub hardening activities.

https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

sarahwells.dev

- The threat actor then accessed Drift's AWS environment and obtained OAuth tokens for Drift customers' technology integrations.

https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

- The threat actor then accessed Drift's AWS environment and obtained OAuth tokens for Drift customers' technology integrations.

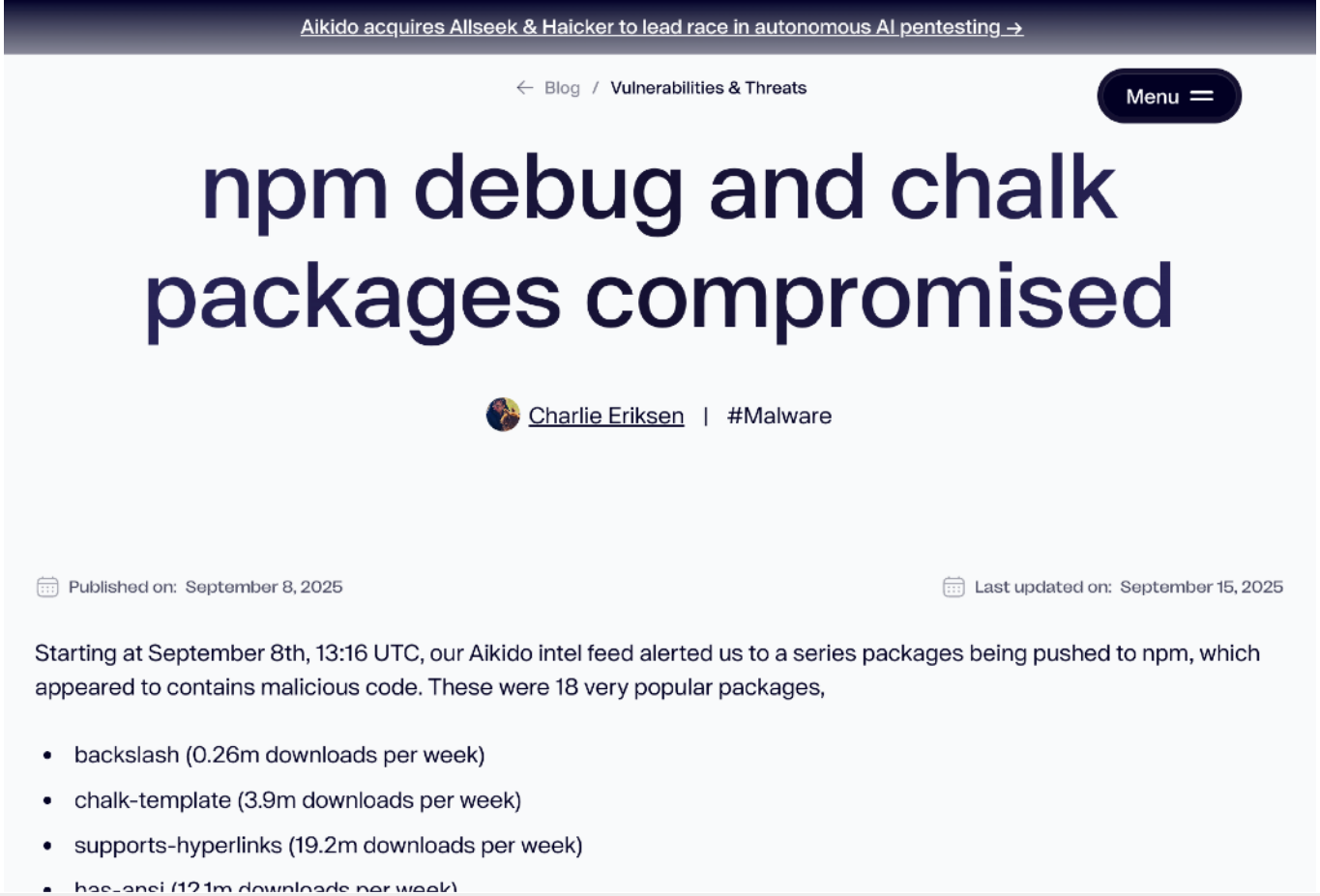
Furthermore, we are implementing new multi-factor authentication processes and further refining limitations to the application environment. These measures are complemented by an ongoing analysis of available logs and configuration settings, as well as the remediation of secrets within the environment and GitHub hardening activities.

https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

sarahwells.dev

Supply chain attack on npm

sarahwells.dev



https://www.aikido.dev/blog/npm-debug-and-chalk-packages-compromised

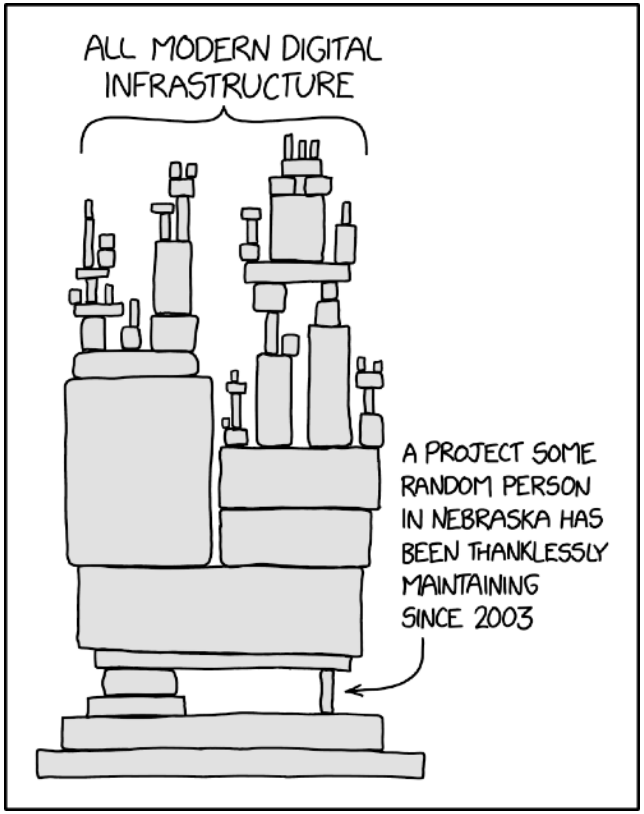
sarahwells.dev

https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

sarahwells.dev

Responding to this breach

Does our code depend on any of the packages?

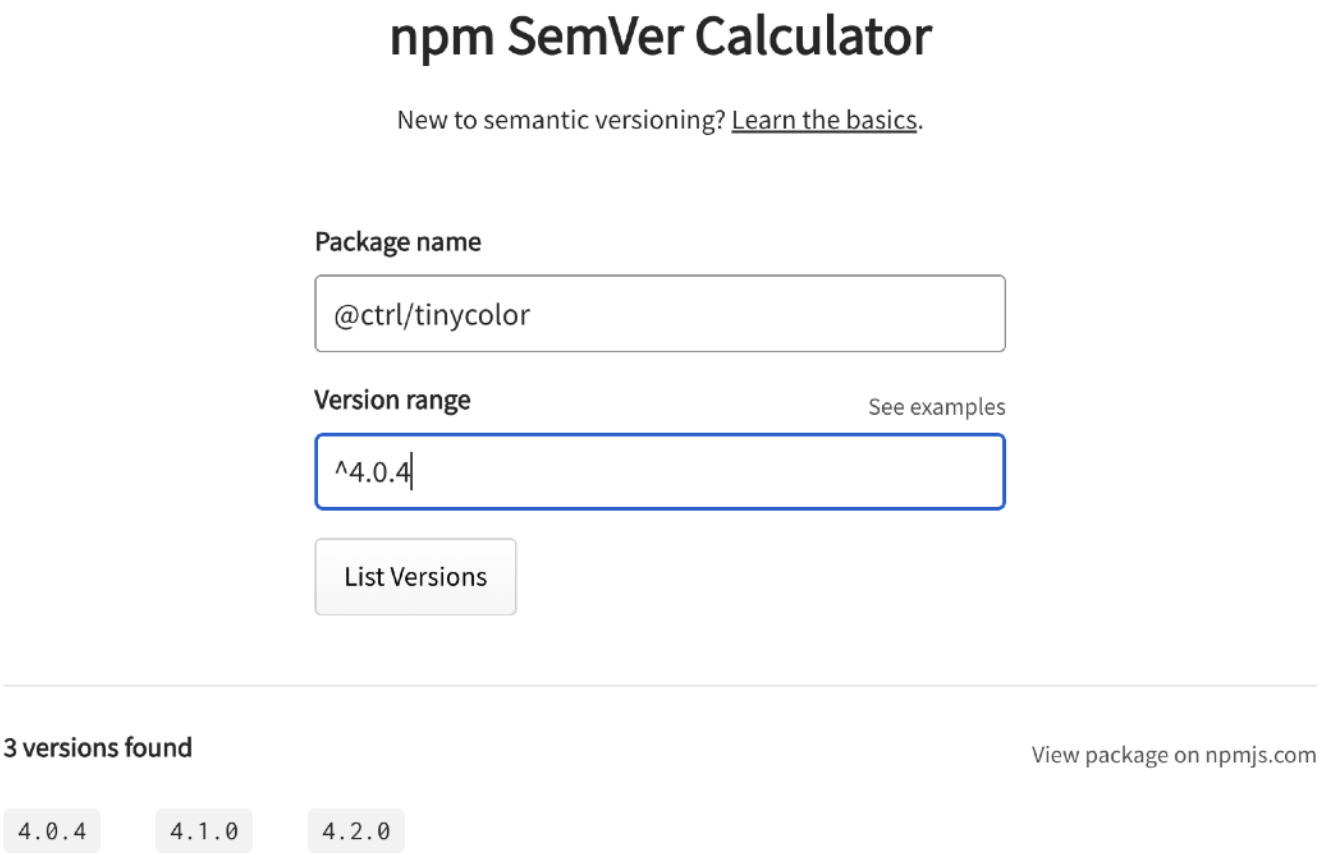


https://xkcd.com/2347/

- Conduct a dependency review of all software leveraging the npm package ecosystem.
  - Check for `package-lock.json` or `yarn.lock` files to identify affected packages, including those nested in dependency trees.

https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

sarahwells.dev



https://semver.npmjs.com/


sarahwells.dev

Did we pull down a compromised version?

Autonomous teams means you don’t know what’s going on

Poor governance costs you

Security issues

Unexpected costs

Impact on delivery

Investing time and effort in the wrong things

We do need governance!

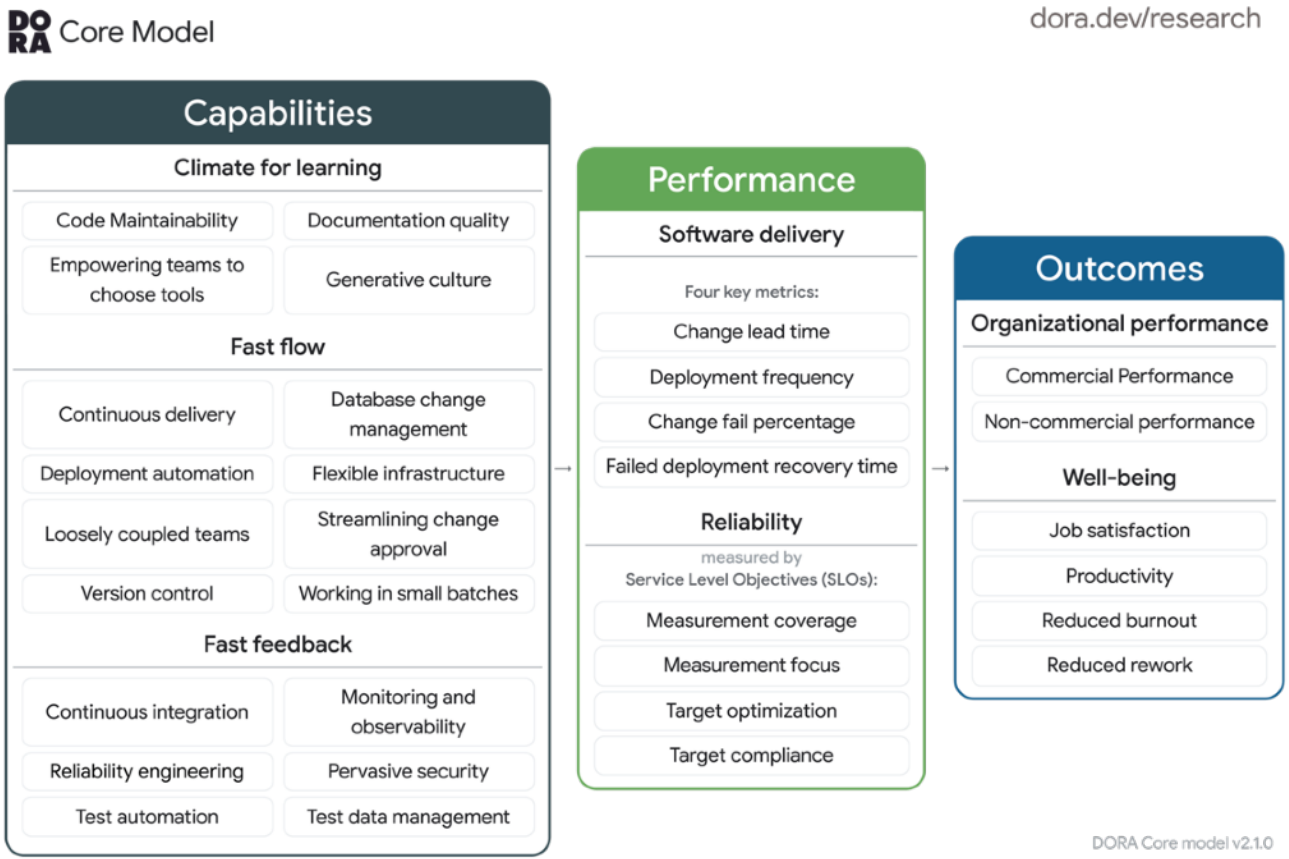
“Governance” has an implementation problem

43 documents you need to read

1. Code of Conduct
2. Software Development Policy
3. Coding Standards and Style Guide
4. Code Review Guidelines
5. Version Control Policy
6. Branching and Merging Strategy
7. Release Management Policy
8. Software Security Policy
9. Data Privacy and Protection Policy
10. Third-Party Library Usage Policy
11. Open Source License Compliance Policy
12. Intellectual Property Policy
13. Software Architecture Standards
14. API Design Guidelines
15. Database Design Standards
16. Testing Policy and Procedures

sarahwells.dev

Let’s look at those DORA core capabilities again



DORA Core, https://dora.dev/research

sarahwells.dev

Bring engineering skills to bear

Governance: a definition

(Software engineering governance)

The set of principles, practices and tools

The set of principles, practices and tools **that help teams**

sarahwells.dev

The set of principles, practices and tools that help teams **make consistent, informed and safe technical decisions**

sarahwells.dev

Good governance is not about saying “no”, it’s about saying “yes”, safely

Good governance allows organisations to move *faster*

The challenges

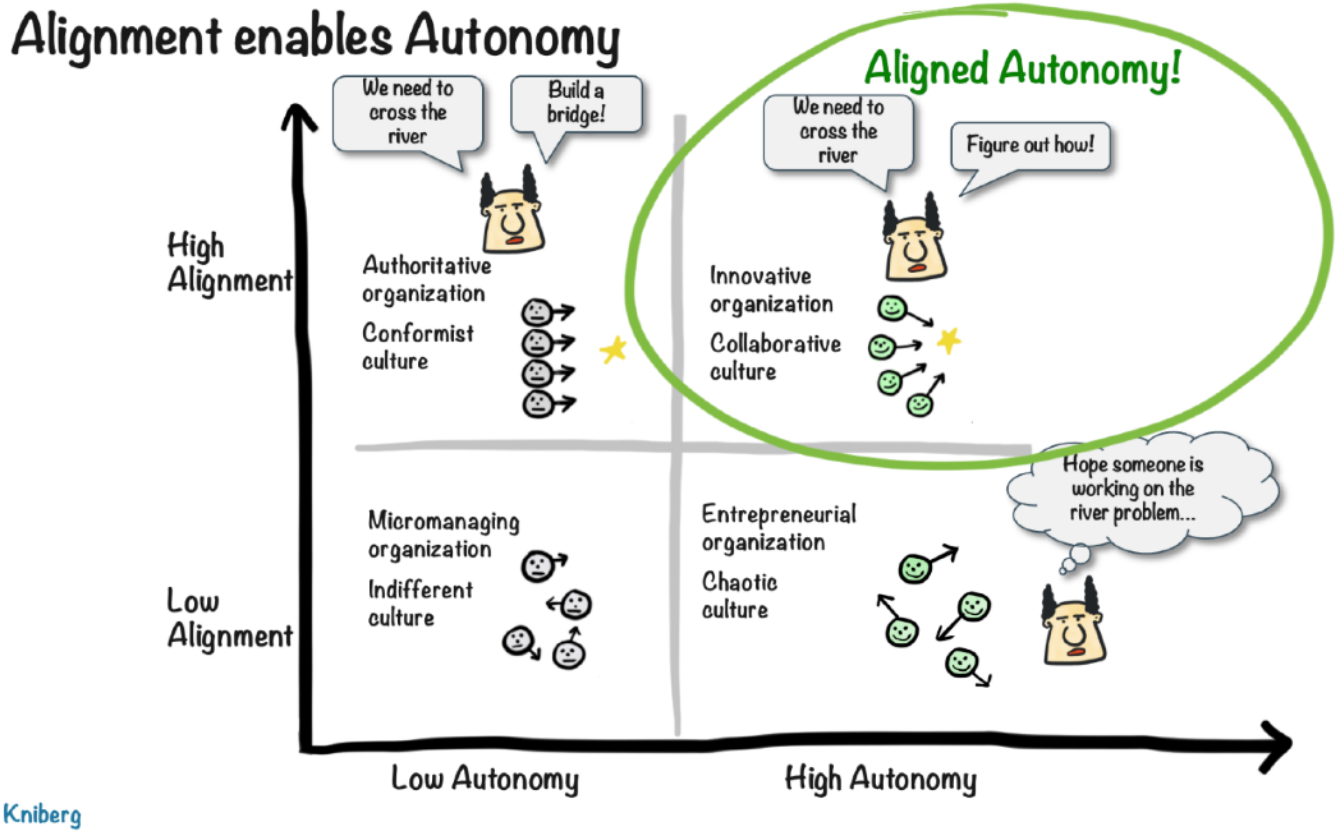
Engineers want to do the right thing

What IS the right thing?

Humans make mistakes

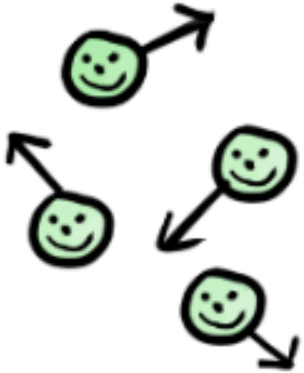
Do the tools and processes catch these mistakes?

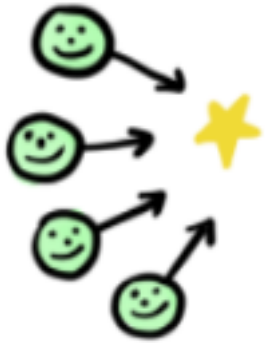
People don’t magically get aligned



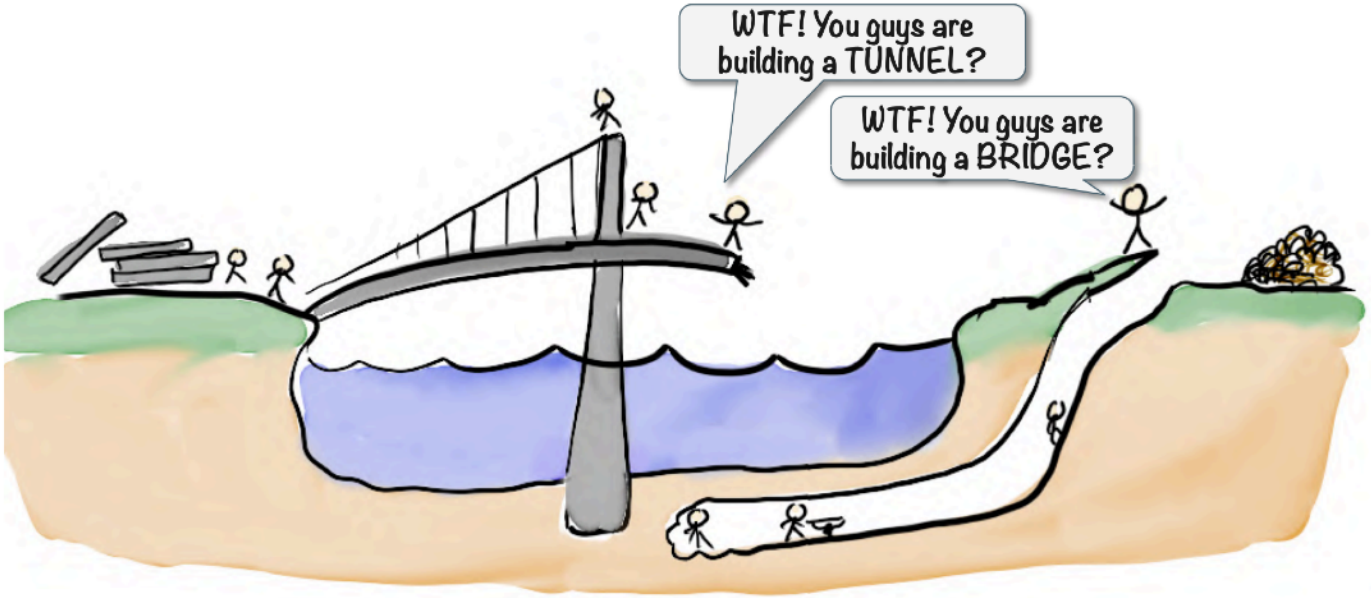
https://blog.crisp.se/2023/09/20/henrikkniberg/agile-intro-slides-from-my-kth-talk

sarahwells.dev





https://medium.com/@hamrinmarcus/another-perspective-on-alignment-autonomy-fb3b2edd4a69



https://blog.crisp.se/wp-content/uploads/2016/08/Agile-Africa-keynote-Alignment-at-Scale.pdf


sarahwells.dev

Modern software estates are complicated

Getting governance right

Foundations

Alignment

Choices

Guardrails

Foundations: Know your software estate

sarahwells.dev

Building your inventory

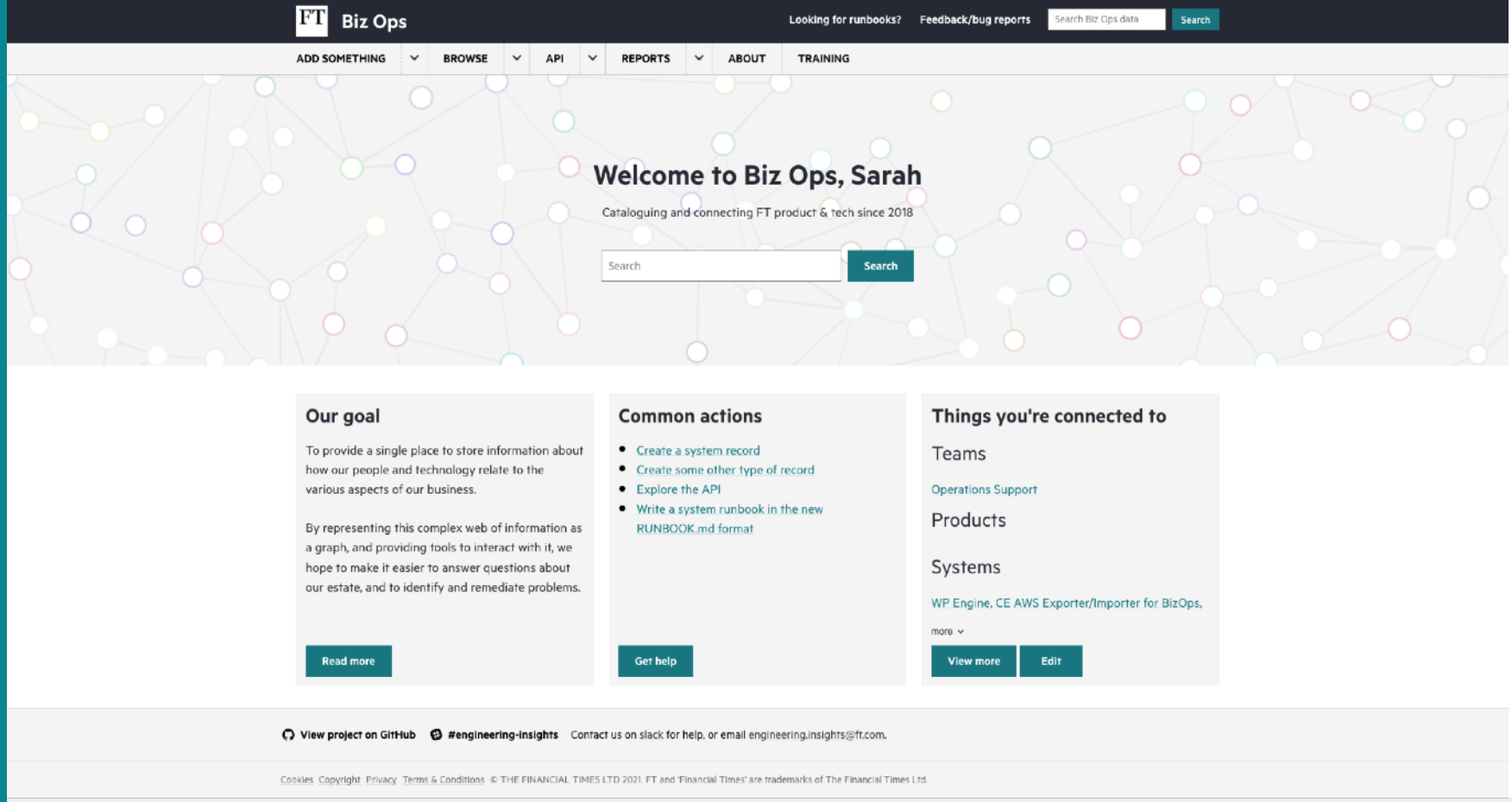
Why do I want an internal developer portal, anyway?

Here's what you actually want: your developers waking up, drinking a cup of coffee, then getting into a flow and spending their day building new features or solving hard business problems.

And here's what you really don't want: your developers waking up, drinking a cup of coffee, then chasing your other developers in order to figure out who owns the service that just broke this other service, only to discover it was maintained by someone who doesn't work here anymore, but wait, someone finally found documentation for it, except never mind, the docs have never been updated, and oh yeah, the whole thing was written in Ruby even though everyone else has been using Node except for that one dude who won't give up on Perl. Aaargh.

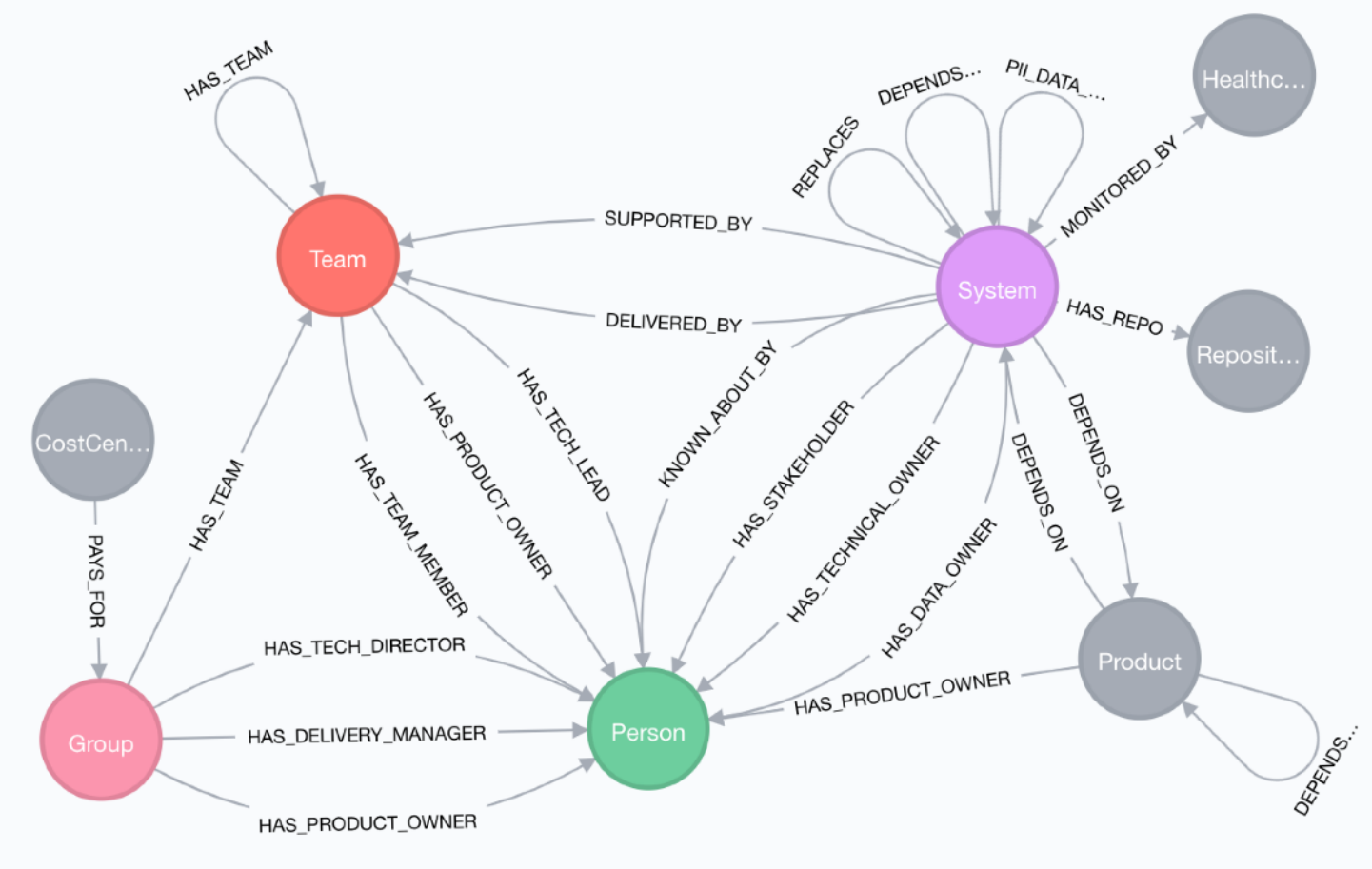
https://backstage.spotify.com/discover/backstage-101/

Start simple



https://www.infoq.com/presentations/productivity-ft/

sarahwells.dev

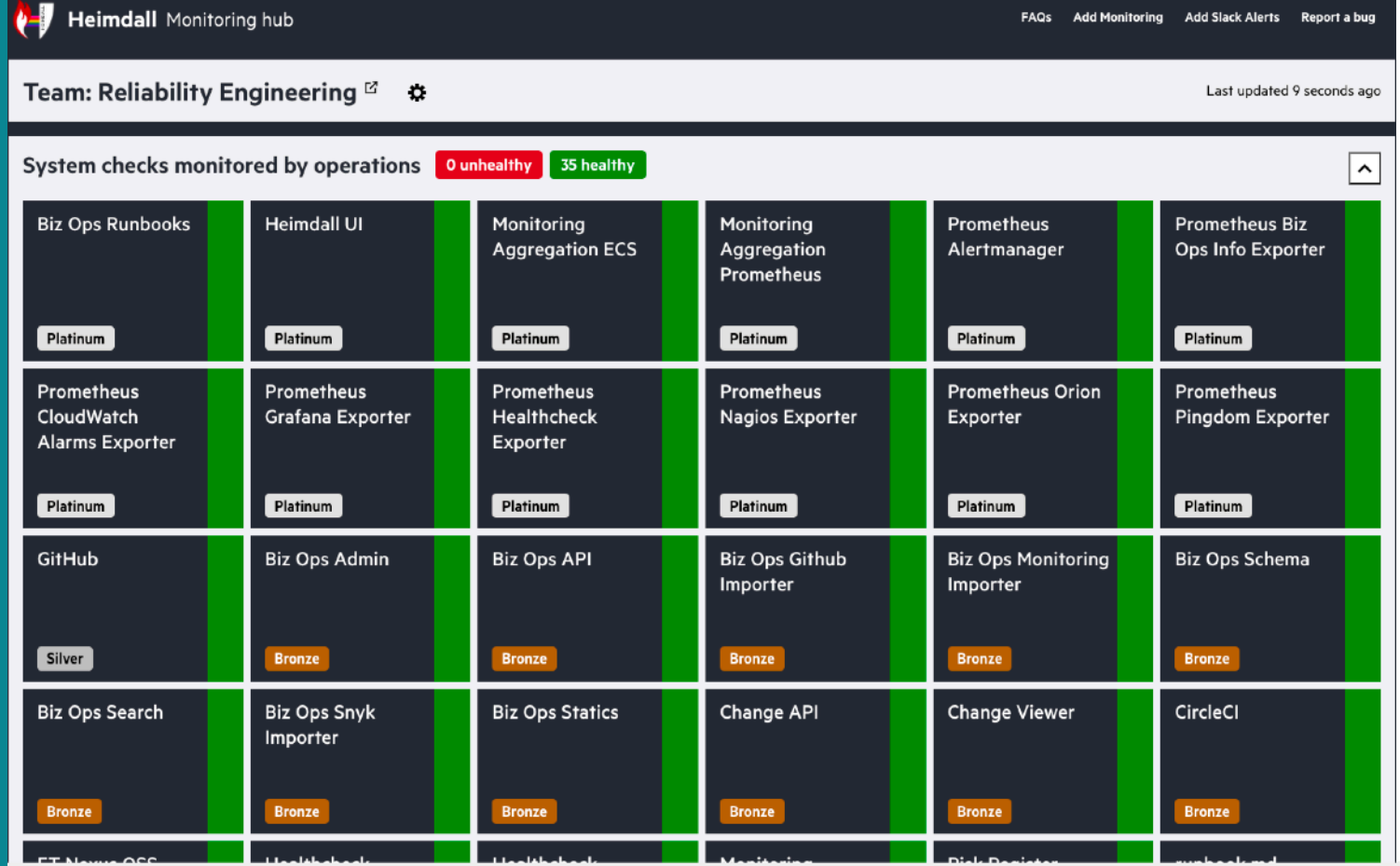


The Biz Ops model

sarahwells.dev

Extending the graph

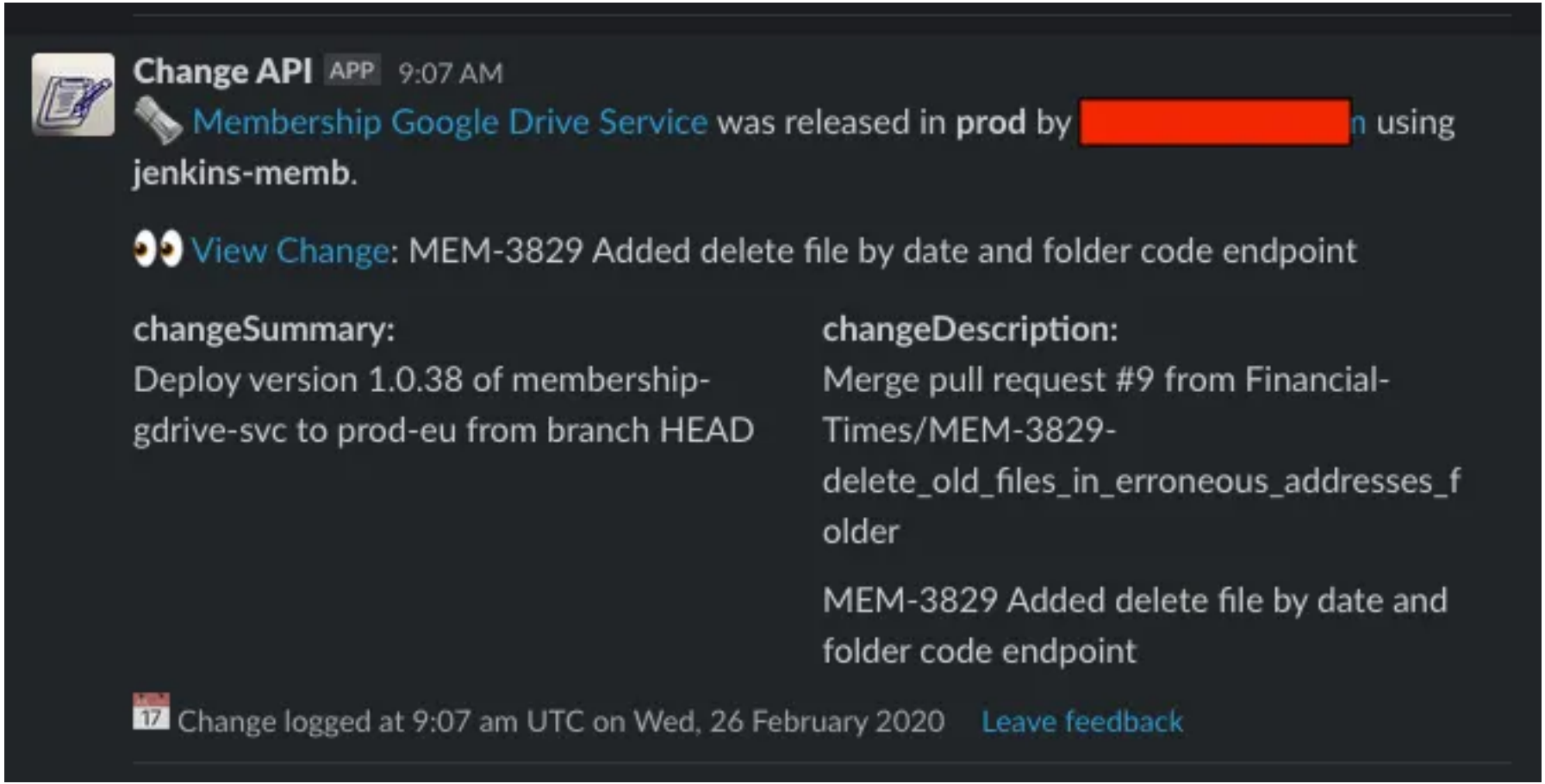
Getting the data


Heimdall Monitoring hub
FAQs
Add Monitoring
Add Slack Alerts
Report a bug
Team: Reliability Engineering
Last updated 9 seconds ago
System checks monitored by operations
0 unhealthy
35 healthy
Biz Ops Runbooks
Platinum
Heimdall UI
Platinum
Monitoring Aggregation ECS
Platinum
Monitoring Aggregation Prometheus
Platinum
Prometheus Alertmanager
Platinum
Prometheus Biz Ops Info Exporter
Platinum
Prometheus CloudWatch Alarms Exporter
Platinum
Prometheus Grafana Exporter
Platinum
Prometheus Healthcheck Exporter
Platinum
Prometheus Nagios Exporter
Platinum
Prometheus Orion Exporter
Platinum
Prometheus Pingdom Exporter
Platinum
GitHub
Silver
Biz Ops Admin
Bronze
Biz Ops API
Bronze
Biz Ops Github Importer
Bronze
Biz Ops Monitoring Importer
Bronze
Biz Ops Schema
Bronze
Biz Ops Search
Bronze
Biz Ops Snyk Importer
Bronze
Biz Ops Statics
Bronze
Change API
Bronze
Change Viewer
Bronze
CircleCI
Bronze

The hardest stuff to find

Making the invisible visible

Track changes too



https://medium.com/ft-product-technology/the-advent-of-change-api-8dae0f95245e

sarahwells.dev

What you get:

✓ Clear picture of current state

✓ An idea of where needs attention

✓ Basis for response - and for automation

Aligning technology decisions

Know the direction of travel

Technology Strategy 2025-2027

1. Cloud-Only Infrastructure

We will migrate entirely to cloud architecture, decommission our data centers, and implement automated CI/CD pipelines to reduce costs by 40% and achieve 99.9% uptime.

2. Unified Data Platform

We will build a modern data lake with real-time analytics and self-service BI tools to accelerate decision-making and enable AI-driven personalization.

3. Digital Customer Experience

We will redesign customer touchpoints with mobile-first, API-driven architecture and AI personalization to improve satisfaction and increase digital engagement.

4. Zero-Trust Security

We will implement comprehensive cybersecurity with zero-trust architecture, AI threat detection, and automated compliance to protect against evolving threats.

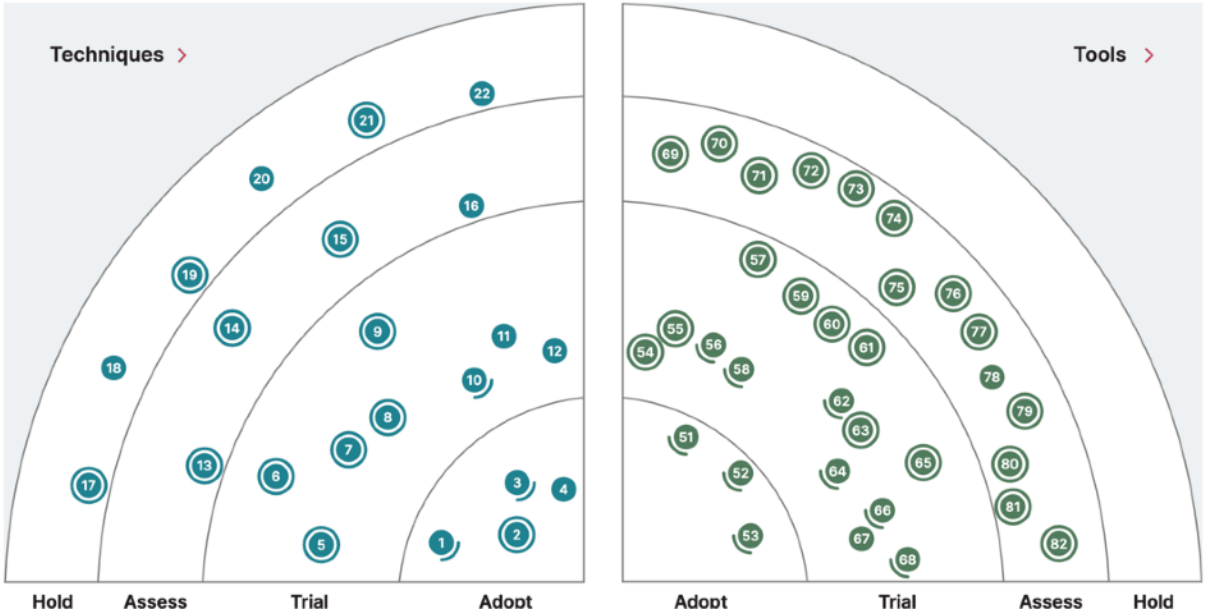
5. AI Integration & Innovation

We will establish AI labs to develop machine learning capabilities, automate business processes, and integrate AI across products to create competitive advantages and new revenue streams.

Building on the strategy

Insights | Search | FAQ | Build your own radar | Archive | Documentary

Thoughtworks Technology Radar is a twice-yearly snapshot of tools, techniques, platforms, languages and frameworks. This knowledge-sharing tool is based on our global teams' experience and highlights things you may want to explore on your projects.



https://www.thoughtworks.com/radar


sarahwells.dev

- Objectively assess what's working, and what isn't
- Pollinate innovation across teams and experiment accordingly
- Balance the risk in your technology portfolio
- Work out what kind of technology organization you want to be
- Set a path for future success

https://www.thoughtworks.com/radar/byor

Zalando Tech Radar

2025.05

Datastores

ADOPT

1. Amazon ElastiCache
2. AWS DynamoDB
3. AWS S3
4. Elasticsearch
5. PostgreSQL

TRIAL

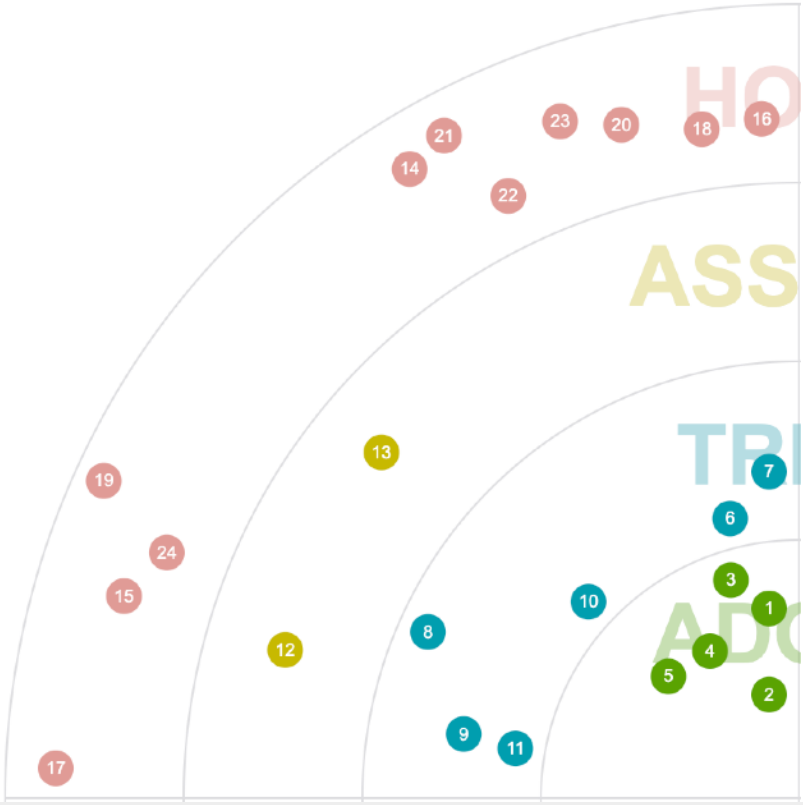
6. Amazon Neptune
7. Amazon Redshift
8. Amazon SageMaker Feature Store
9. AWS DocumentDB
10. Druid
11. HDFS

ASSESS

12. Amazon MemoryDB
13. Valkey

HOLD

14. Apache Cassandra
15. Consul
16. Hazelcast
17. HBase
18. Memcached
19. MongoDB
20. MySQL
21. Oracle DB
22. Redis
23. Solr
24. ZooKeeper



https://opensource.zalando.com/tech-radar/

sarahwells.dev

Communication and knowledge sharing

Summary

Issue

We need to store secrets, such as passwords, private keys, authentication tokens, etc.

Some of the secrets are user-oriented. For example, our developer wants to be able to use their mobile phone to look up a password to a service.

Some of the secrets are system-oriented. For example, our continuous delivery pipeline needs to be able to look up the credentials for our cloud hosting.

Decision

Bitwarden for user-oriented secrets

Vault by HashiCorp for system-oriented secrets.

Status

Decided. We are open to new alternatives as they arise.

Details

Assumptions

For this purpose, and our current state, we value user-oriented convenience, such as usable mobile apps.

- We want to ensure fast easy access on the go, such as for a developer doing on-call system reliability engineering.

https://github.com/joelparkerhenderson/architecture-decision-record/tree/main/locales/en/examples/secrets-storage

What you get:

- ✓ People can make decisions
- ✓ Less duplication of effort
- ✓ Fewer surprises

Making smart technology choices

sarahwells.dev

The allure of shiny and new

The case for boring technology

Dan McKinley
https://mcfunley.com/choose-boring-technology

sarahwells.dev

When to break the boring rule

Developing a culture of thoughtful adoption

Innovation to support business outcomes

The impact on governance itself

What you get:

- ✓ Innovation in the right places
- ✓ Standardisation for everything else
- ✓ Plans, not chaos

Building guardrails that work

sarahwells.dev

Guardrails vs policies vs standards

✅ Policy

A high-level statement of intent or principle, usually approved by leadership.

Purpose: Explains what must be done and why

Characteristics:

- Broad, overarching, and strategic
- Often technology-agnostic
- Non-negotiable: everyone must follow it

Example:

“All production systems must be backed up daily and backups must be retained for at least 30 days.”

📏 Standard

A set of specific, detailed rules or requirements that operationalize the policy.

Purpose: Explains how the policy is met, often with technical details.

Characteristics:

- More specific and measurable
- Often define technical configurations, frequency, or thresholds
- Can vary by environment or system

Example (to support the backup policy):
“All production databases must use vendor-supported snapshot backups scheduled at midnight UTC, with retention set to 35 days.”

Guardrail

A control that guides behaviour to keep it in line with policies or standards.

Purpose: Keeps teams aligned to policies without needing constant manual review.

Characteristics:

- Often built into tools
- Can be preventive (blocking unsafe changes) or detective (alerting on drift)
- Balance: tight enough to protect, loose enough to allow innovation

Example:
“A spending alert that triggers when monthly spend exceeds 80% of the forecasted budget.”

✅ In summary:

	What	Example
Policy	High-level rule	“All data must be encrypted at rest.”
Standard	Detailed, actionable requirement	“Use AES-256 encryption for all databases.”
Guardrail	Check or control	“Prevent deployment of storage without encryption enabled.”

Make the right thing the easy thing

1. Buy vs Build

Can you buy something to solve this problem rather than building it?

2. Procurement

We need to go through a procurement process for any new relationship with a supplier, whether free or paid

3. TGG Endorsement

Changes to the way the FT uses technology should be raised at the Tech Governance Group

4. Adding to Biz Ops

Make sure the initial record has been created

5. Security & Privacy

We need to build secure products and services

6. Accessibility & Browser Support

We need to build websites that meet the needs of our customers

7. Analytics, Logs & Metrics

We need to make sure we know how the things we built are used

8. Change & Release Logging

All changes made at the FT must be logged

9. Healthchecks & Monitoring

Make sure people can tell whether your system is up and working as expected

10. Runbooks

Could someone else fix a problem with your service

11. Service Tier & Support

Is this brand or business critical or could we wait til the morning to fix it?

12. Performance

How would you know if performance started to tank?

13. Cost Management

Are you paying over the odds for this?

14. Going Live

How to take your system live

15. While the Service is Live

Maintaining your service

16. Decommissioning

How to turn your service off

The FT's Engineering Checklist

sarahwells.dev

4. Adding to Biz Ops

Make sure the initial record has been created

You needed to do this to spin up AWS resources

4. Adding to Biz Ops

Make sure the initial record has been created

Build in flexibility for legitimate exceptions

10. Runbooks

Could someone else fix a problem with your service

FT System Operability Score powered by Biz Ops

ALL GROUPS | TEAM LEAGUE TABLE | SYSTEM LEAGUE TABLE | PRODUCT LEAGUE TABLE | ABOUT

ALL GROUPS > ENGINEERING ENABLEMENT > RELIABILITY ENGINEERING > PROMETHEUS-GRAFANA-EXPORTER

System: prometheus-grafana-exporter

Platinum Production

Score: 91% Rescore Score updated: October 1 2021

Rated Green by Ops, August 5 2021

Bear in mind that the scoring rules are a work in progress. In some cases (particularly with regard to third party systems) they won't always make perfect sense, so use your discretion. Not getting 100% is normal for now. Fixing all the things you know how to fix is the main thing to aim for.

Fix these errors in BizOps | View runbook | New here? Find out what to do next

Runbook aspect	Status	Failings	Remedial actions
dependencies	Error	Error: Dependency on ft-grafana, which is marked as discontinued - that can't be right! Critical: Dependency on ft-grafana, of lower service tier Gold, is an operational risk. If you employ some architectural pattern to improve resilience, please add details https://github.com/Financial-Times/biz-ops-admin/blob/master/docs/dependency-details.md	-
failover	Error	Error: FailoverDetails is not allowed to be empty	-
architecture	Error	Error: Architecture is not allowed to be empty Warning: Architecture is not allowed to be empty Info: Architecture is not allowed to be empty	-
moreInformation	Warning	Warning: MoreInformation is not allowed to be empty Info: MoreInformation is not allowed to be empty	-
replaces	Info	Info: Replaces is not specified	-
knownAboutBy	Info	Info: KnownAboutBy is not specified	-
firstLineTroubleshooting	Info	Info: FirstLineTroubleshooting contains links	-
basicDetails	OK	None	-
hostPlatform	OK	None	-
dependents	OK	None	-

sarahwells.dev

Automation is your friend

What you get:

✓Catch problems early

✓Clarity of what good looks like

✓Flexibility where needed

Conclusions

From bottleneck to enabler

Good governance is largely invisible to developers in their day-to-day work

Good governance is largely invisible to developers in their day-to-day work, **manifesting as helpful automation, clear guidelines, and self-service tools that make the right choices the easy choices**

Foundations

Alignment

Choices

Guardrails

https://sarahwells.dev