Leveraging Governance inside your Microsoft Fabric Tenant and Workspace

Martin Catherall

Heidi Hasting

Agenda

- What is Governance
- Why it fails
- Governance Foundations in Fabric
- Data Mesh
- Fabric Settings and functionality to aid governamce
  - Tenant
  - Domain
  - Workspace
- Auditing and Monitoring

What is governance

- Data governance is the framework of policies, processes, and standards that organizations use to manage their data assets effectively. It ensures data is accurate, consistent, secure, and accessible to the right people at the right time. A strong data governance strategy defines who owns data, how it's collected, stored, and used, and who is accountable for its quality. It helps organizations comply with regulations like GDPR and HIPAA, reduces risks associated with data breaches, and builds trust among stakeholders. As data volumes grow, good governance becomes essential for making informed business decisions and maintaining a competitive edge in the digital age.
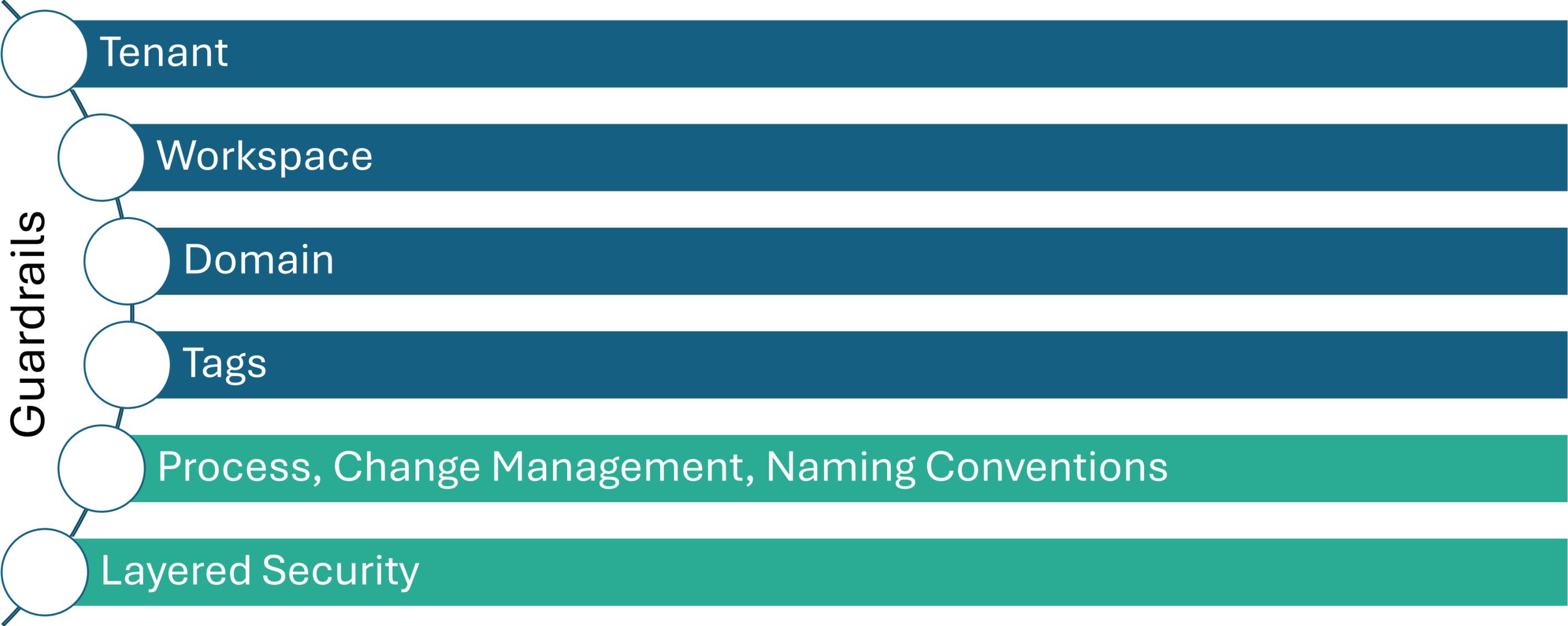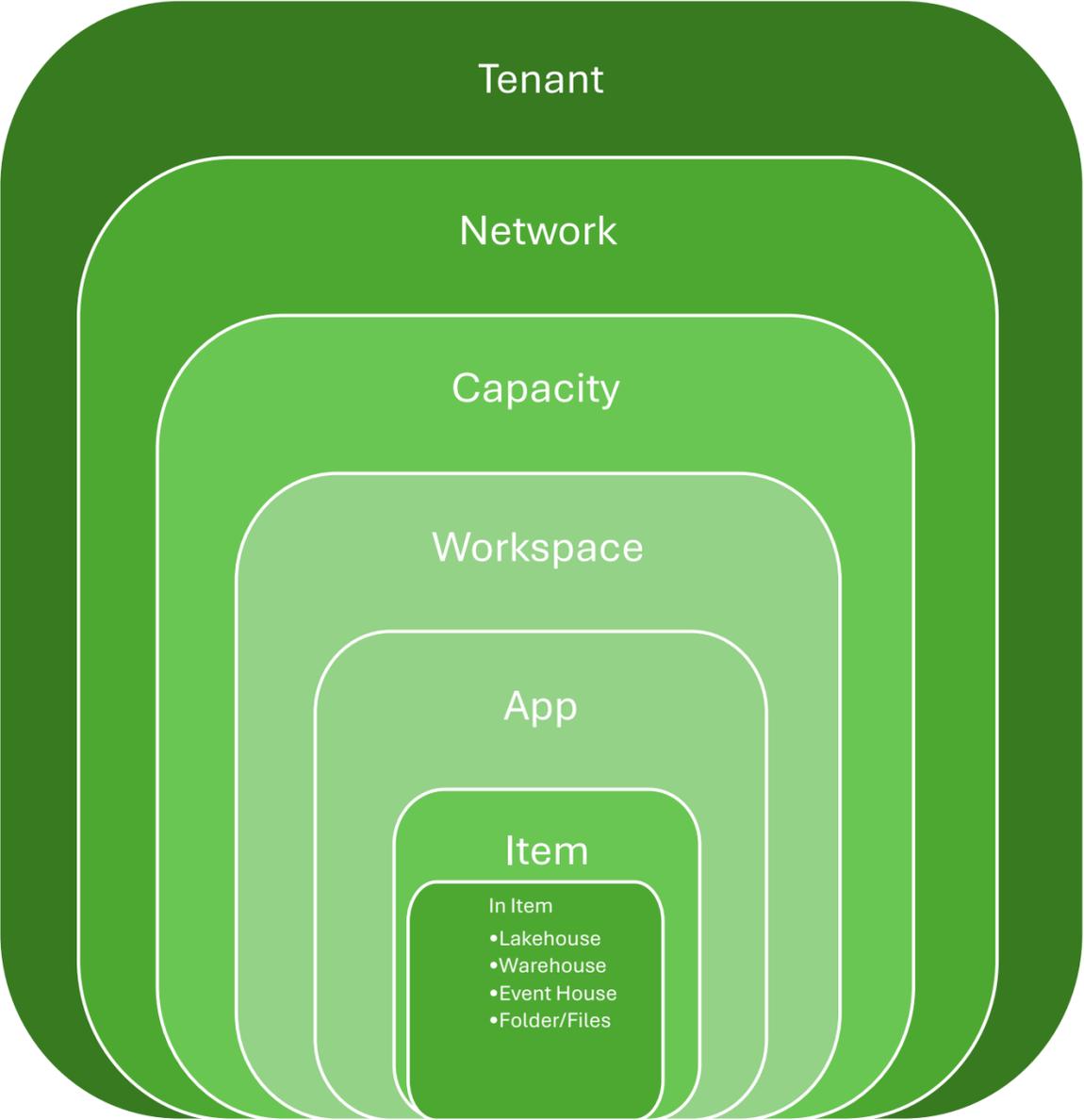
Why it fails?

- Settings Configured in Isolation
- Fabric Tenant settings are configured reactively instead of proactively
- IT lockdown vs free for all
  - Shadow IT
  - Nobody knows who owns it
- Workspaces
  - without naming conventions
  - no owner or purpose

Governance Foundations in Fabric

Guardrails

- Tenant
- Workspace
- Domain
- Tags
- Process, Change Management, Naming Conventions
- Layered Security

Governance Foundations in Fabric – Security Layers

Governance

Documentation

Task Flows

Standards

Process

Define

Design

Request

Approve/Reject

Action

Automate

Change Management

Owners

Security

Item level

Row Level, Column Level, Object level

Audit

Sensitivity

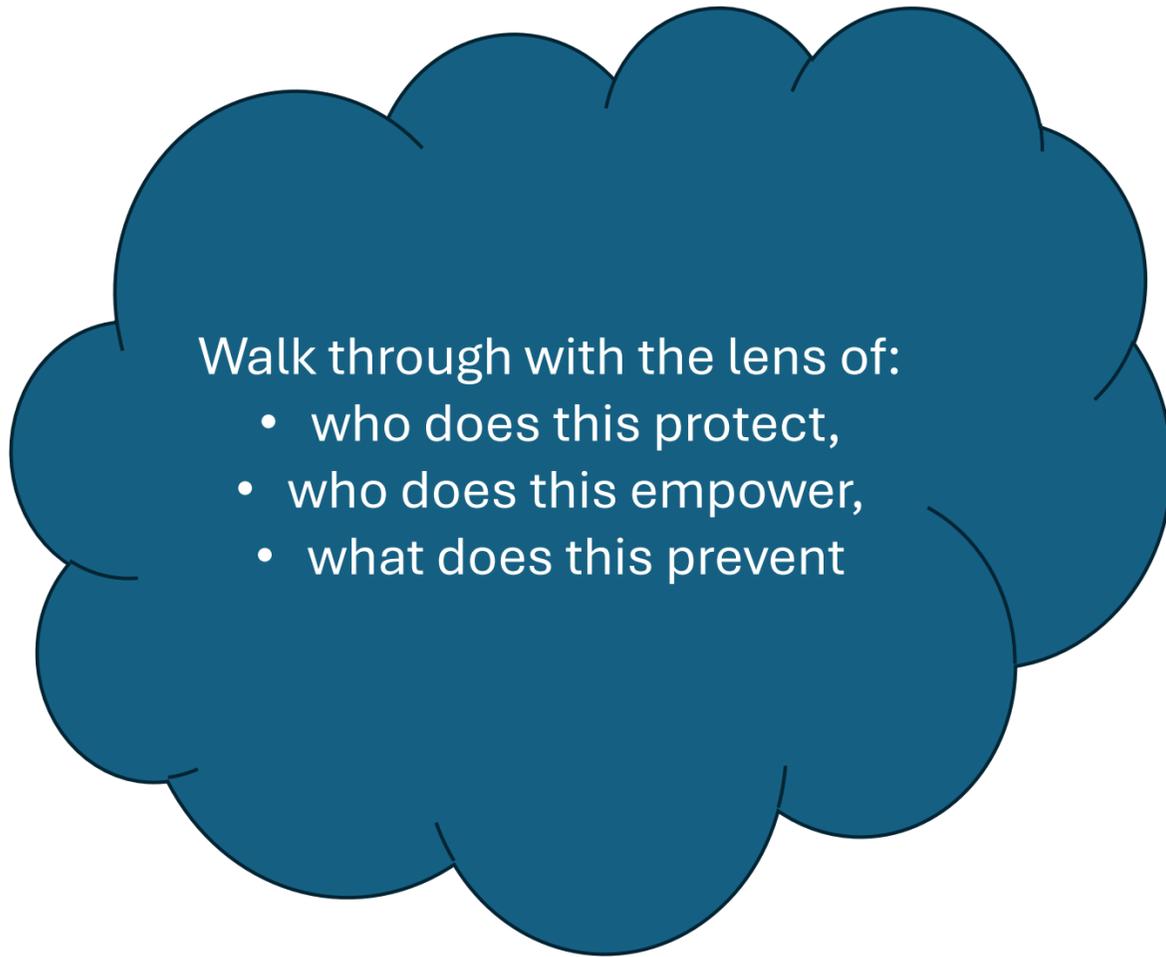Access

Who/What/When/Where/Why

Monitor

Data Mesh

- **Data Mesh empowers domains** to own, model, and publish high-quality data products.

- **Data Governance provides the guardrails**—policies, lineage, quality, security, and lifecycle controls.

- **Microsoft Fabric unifies both**, enabling domain-driven data products governed by a central,

  consistent foundation (OneLake, Purview, security, cataloguing).

Result: **Scalable, federated data architecture with enterprise-grade governance.**

Tenant-Level settings – The Overlooked Ones

- Fabric Item creation
- Copilot and AI settings
- Publish to Web
- Domains
- Information Protection / Sensitivity Labels
- External sharing and guest access

- Management of Tenant Settings
  - Tracking changes
  - Keeping track of the 100+ settings (and growing…)

Walk through with the lens of:
- who does this protect,
- who does this empower,
- what does this prevent

Rule of thumb: every setting should have a documented "why" behind it, not just an on/off state

Domains – Your Data Mesh Backbone

- Way to define a logical grouping
  - Finance
  - HR
  - Sales
  - Operations
  - Audit
- Defined at Tenant
  - Default security....
- Attached to workspace

- **Demo 1**

Workspace Settings – Governance at the Coal Face
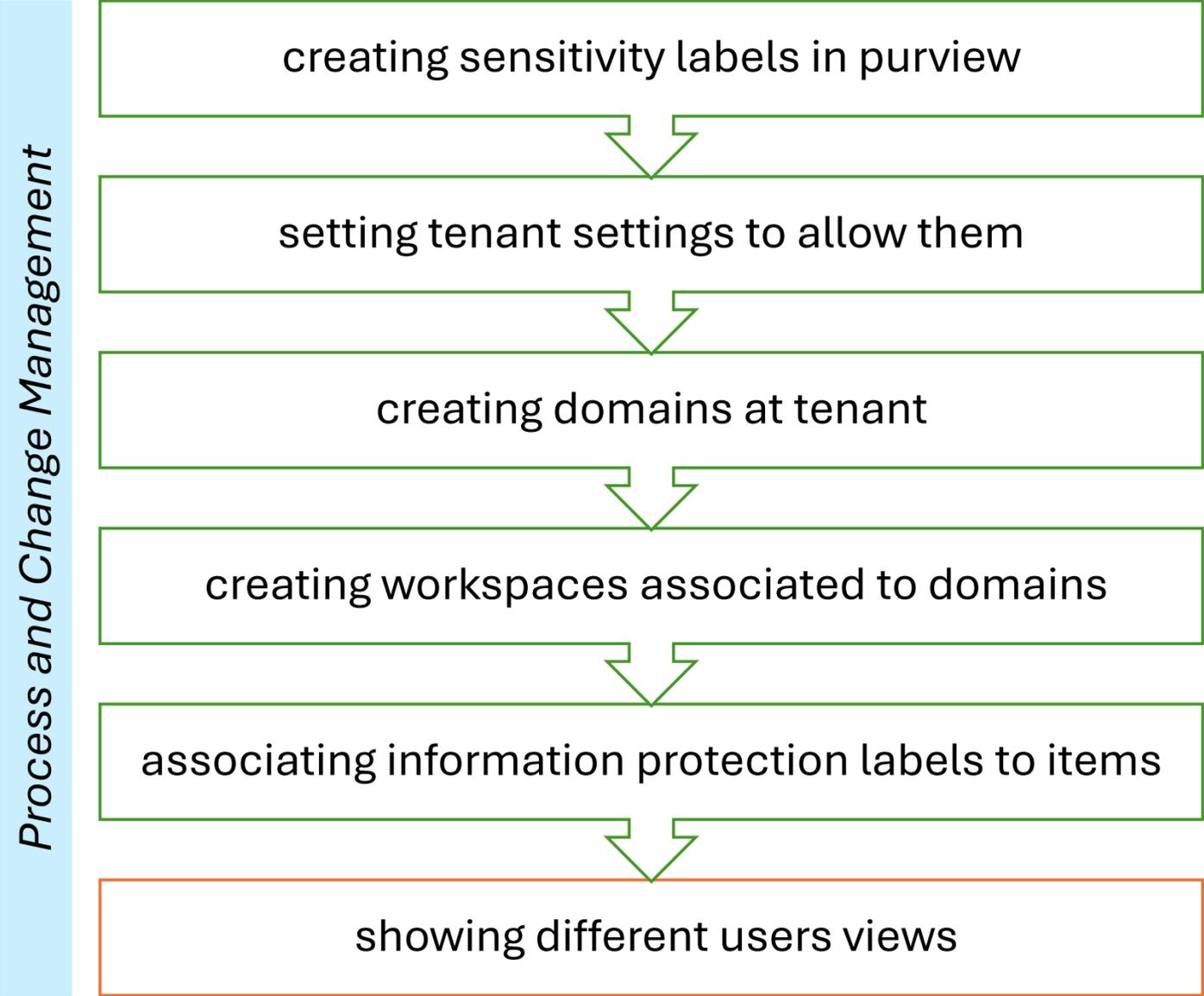
- **What Workspace Admins CAN Control**
- Who has access and at what role — Admin, Member, Contributor, Viewer
- Endorsement nominations — they can promote content to Promoted status themselves
- OneDrive integration and Git integration (if enabled at tenant)
- Contact list — who gets notified when something goes wrong

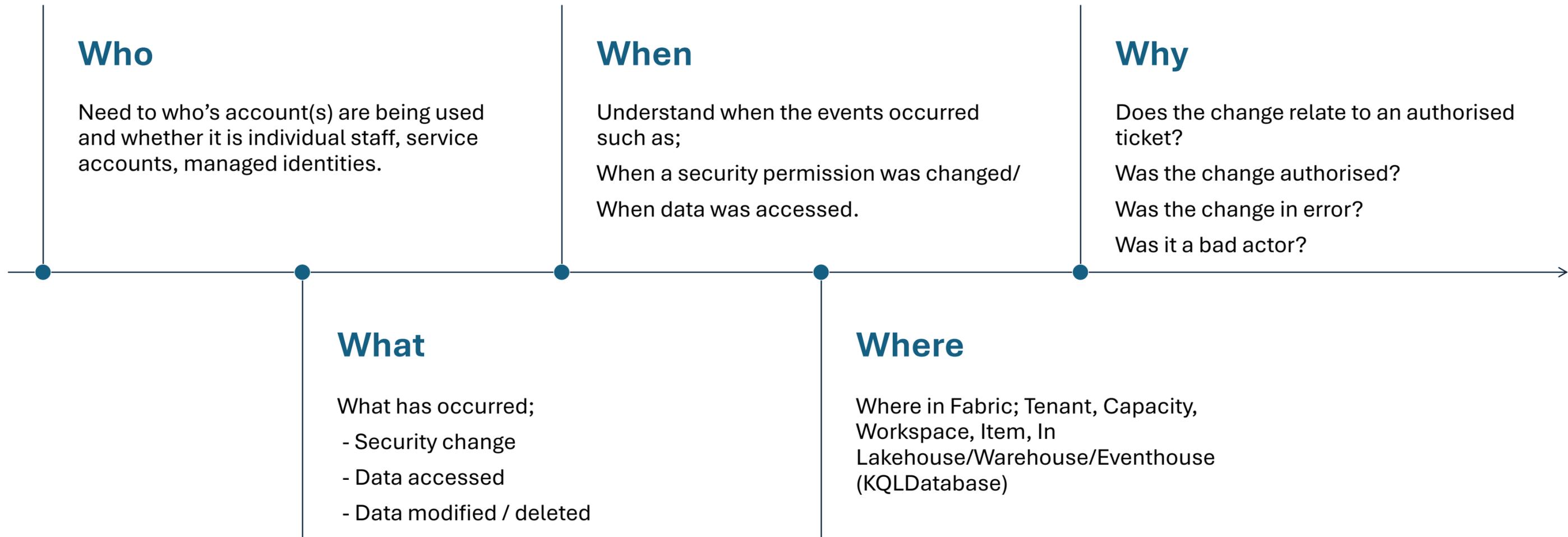- **What Workspace Admins CANNOT Control**
- They cannot override tenant-level sharing restrictions
- They cannot certify content — certification requires a designated certifier set at tenant level
- They cannot change the domain their workspace belongs to
- They cannot disable mandatory sensitivity labelling if enforced at tenant
- They cannot grant themselves more permissions than their own role allows

Putting it All Together – A Governance Blueprint

Demo 2

Process and Change Management

- creating sensitivity labels in purview
- setting tenant settings to allow them
- creating domains at tenant
- creating workspaces associated to domains
- associating information protection labels to items
- showing different users views

Audit

Who

Need to who's account(s) are being used and whether it is individual staff, service accounts, managed identities.

When

Understand when the events occurred such as;

When a security permission was changed/

When data was accessed.

Why

Does the change relate to an authorised ticket?

Was the change authorised?

Was the change in error?

Was it a bad actor?

What

What has occurred;

 - Security change

 - Data accessed

 - Data modified / deleted

Where

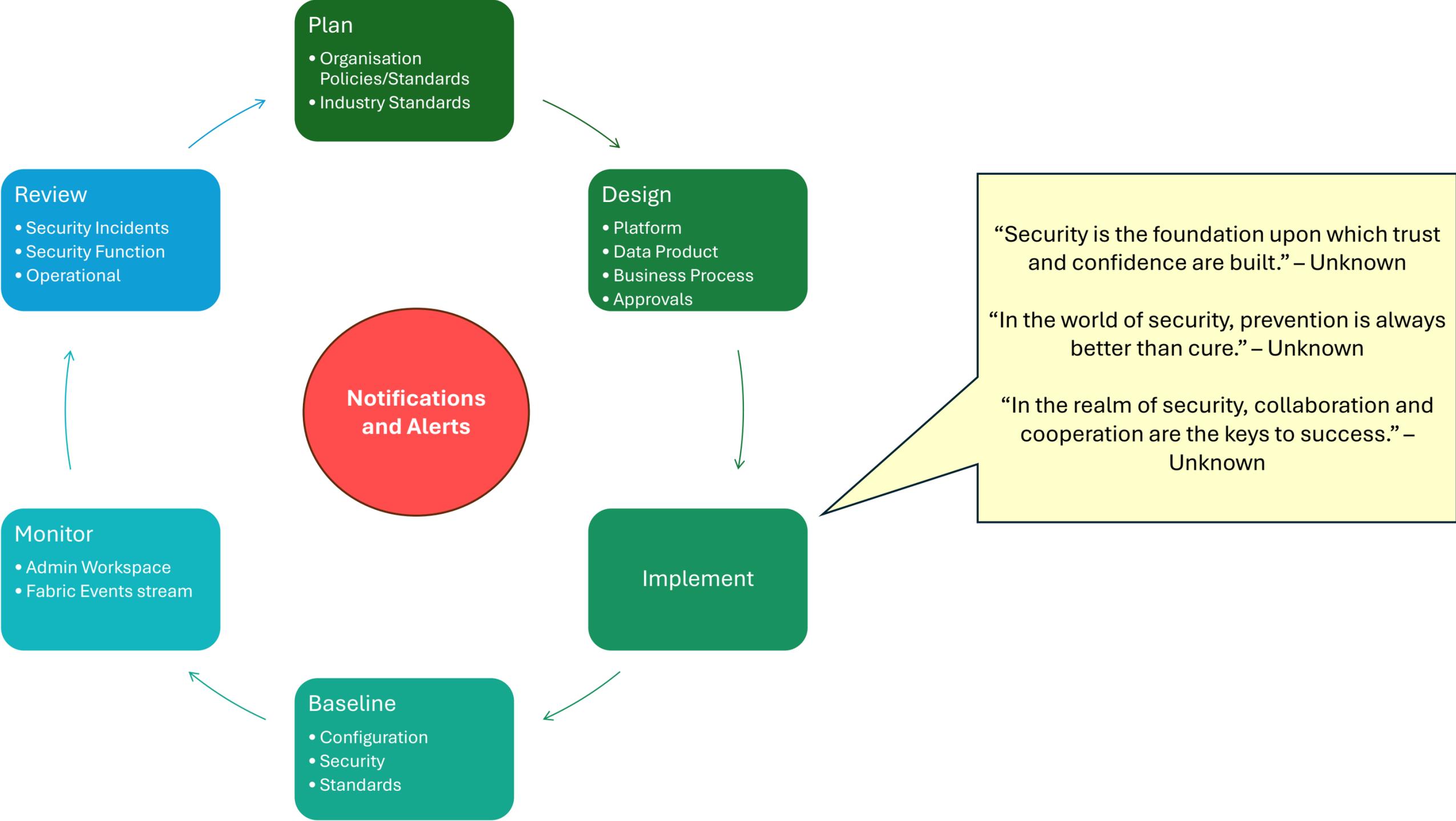Where in Fabric; Tenant, Capacity, Workspace, Item, In Lakehouse/Warehouse/Eventhouse (KQLDatabase)

Monitoring

Summary

Sound off.
The mic is all yours.
Influence the product roadmap.

Join the Fabric User Panel

Share your feedback directly with our Fabric product group and researchers.

https://aka.ms/JoinFabricUserPanel

Join the SQL User Panel

Influence our SQL roadmap and ensure it meets your real-life needs

https://aka.ms/JoinSQLUserPanel

Microsoft Fabric governance - Microsoft Fabric | Microsoft Learn

FABCON SQLCON

ATLANTA26   JOIN THE CONVERSATION #FABCONSQLCON26

Sound off.
The mic is all yours.
Influence the product roadmap.

Join the Fabric User Panel

Share your feedback directly with our Fabric product group and researchers.

https://aka.ms/JoinFabricUserPanel
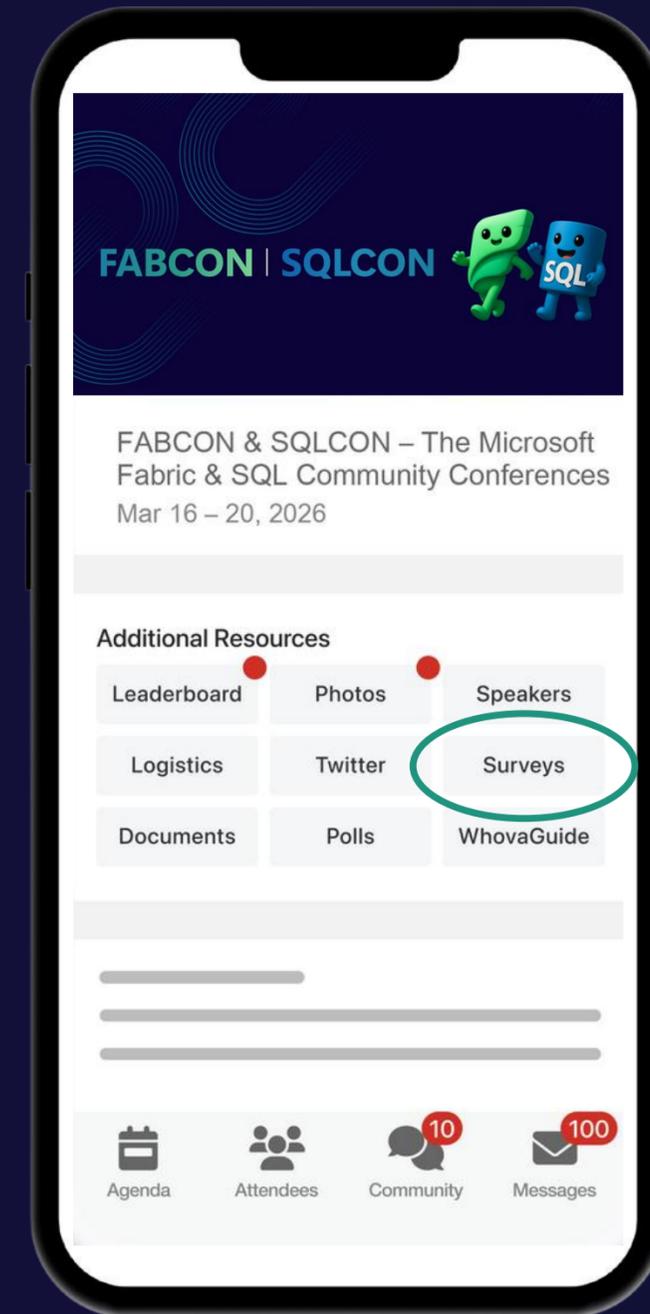
Join the SQL User Panel

Influence our SQL roadmap and ensure it meets your real-life needs

https://aka.ms/JoinSQLUserPanel
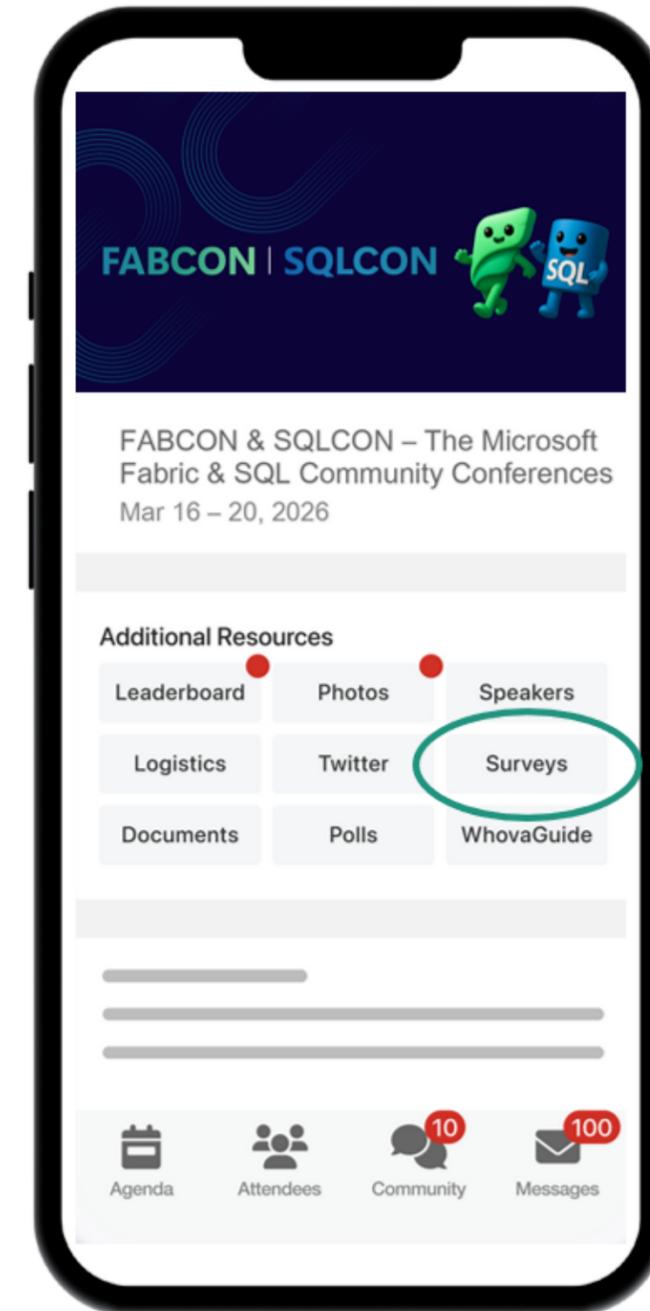
Get Two Fabric Certifications for FREE

Attendees of FABCON can take the Fabric Analytics Engineer or Fabric Data Engineer exam for free. Be part of the 2 fastest growing role-based certifications in Microsoft history.

Request your voucher by March 23, 2026.

https://aka.ms/fabcon/cert100

Microsoft Certified
Associate