ENTERPRISE FRAMEWORK · TELECOM EXPENSE MANAGEMENT

TEM Security Control Framework

A practical tool for evaluating control maturity across telecom data, workflows, and oversight

Use this framework to assess how well your organization is strengthening control over sensitive telecom data and related processes. For each statement, mark **Established, Developing, or Needs Attention.**

1 ACCESS AND ROLE DISCIPLINE

- ☐ Access to telecom billing, contract, inventory, and service data is assigned according to defined roles and business need.
- ☐ User permissions are reviewed regularly and updated when responsibilities change.
- ☐ Privileged or sensitive access is limited to the smallest practical group of users.
- ☐ Third-party access is governed by clear approval and review practices.

2 DATA GOVERNANCE AND HANDLING

- ☐ Sensitive telecom records are classified and handled according to clear internal standards.
- ☐ Exports, reports, and shared files follow controlled processes rather than ad hoc distribution.
- ☐ Teams use approved methods for sharing telecom-related data across departments and vendors.
- ☐ Sensitive records are retained, stored, and managed consistently across workflows.

3 WORKFLOW CONTROL AND DOCUMENTATION

- ☐ Telecom approvals, disputes, account changes, and service updates follow repeatable processes.
- ☐ Key workflow actions are documented clearly enough to support accountability and review.
- ☐ Manual handoffs are limited where possible or managed through defined control steps.
- ☐ Reporting and approvals are structured to reduce reliance on unmanaged spreadsheets and email attachments.

4 INVENTORY AND SYSTEM VISIBILITY

- ☐ The organization maintains a reliable system of record for telecom services, assets, and related data.
- ☐ Inventory, billing, account, and service records can be reconciled with reasonable confidence.
- ☐ Teams can identify what services are active, where they are deployed, and who owns them.
- ☐ Lifecycle changes such as adds, moves, disconnects, and updates are reflected consistently in records.

5 OWNERSHIP AND ACCOUNTABILITY

- ☐ Ownership of telecom data, workflows, and reporting is clearly assigned.
- ☐ Responsibilities across finance, IT, procurement, telecom operations, and other stakeholders are understood.
- ☐ Escalation paths exist for telecom security, control, and data-governance issues.
- ☐ Control responsibilities are reviewed often enough to stay aligned with operational changes.

6 VENDOR AND OVERSIGHT PRACTICES

- ☐ Vendors, carriers, and service providers are expected to follow defined security and governance practices.
- ☐ Telecom-related third-party workflows are monitored with appropriate oversight.
- ☐ Contracted relationships support accountability for handling sensitive telecom information.
- ☐ Telecom controls are aligned with broader enterprise governance and oversight expectations.

© 2026 Tellennium I For informational purposes only.

HOW TO INTERPRET YOUR RESULTS

Mostly Established

Your organization likely has a stronger control posture and a more disciplined approach to telecom governance.

Mix of Established and Developing

Key control practices are taking shape, but important weaknesses may still limit oversight and consistency.

Frequent Needs Attention

Your environment may need stronger structure around access, governance, workflow control, inventory visibility, and accountability.

Stronger telecom security depends on more than awareness of risk. It requires consistent control disciplines that improve visibility, accountability, and governance across the telecom environment. This framework can help identify which of those disciplines deserve the most attention next.

© 2026 Tellennium I For informational purposes only.