Pragmatic GRC™

F-004
Governance Roles & Responsibilities

Foundation Resource | Version 1.0 | Practical Implementation Guide

Document Information

Field	Value
Resource ID	F-004
Resource Family	Foundation
Related Chapters	4, 5, 8
Related Resources	F-001, F-002, F-003, G-002, H-001
Version	1.0
Status	Initial Release

Executive Summary

Successful governance depends on clearly defined accountability. This guide helps organizations assign GRC responsibilities to existing personnel without creating unnecessary bureaucracy.

Purpose

Define ownership for governance, risk management, cybersecurity, and compliance activities and establish accountability for maintaining the Three Living Documents and recurring governance processes.

Governance Operating Model

Executive Leadership

▼

Program Sponsor

▼

Business Owners

▼

IT / MSP

Employees

Executive Sponsor

Provides strategic direction, approves major risks, reviews governance metrics, and champions the GRC program.

✓ **Best Practice:** Assign responsibilities to existing positions whenever possible.

Business Owner

Owns business assets, approves operational changes, identifies risks, and participates in the Monthly GRC Heartbeat™.

✓ **Best Practice:** Assign responsibilities to existing positions whenever possible.

IT / Managed Service Provider

Maintains technical controls, identity management, backups, patch management, and system security.

✓ **Best Practice:** Assign responsibilities to existing positions whenever possible.

Department Managers

Promote governance practices, ensure policy compliance, and escalate operational issues.

✓ **Best Practice:** Assign responsibilities to existing positions whenever possible.

Employees

Follow policies, protect assets, report incidents, and complete required awareness training.

✓ **Best Practice:** Assign responsibilities to existing positions whenever possible.

Governance Responsibility Matrix

Activity	Executive	Business Owner	IT/MSP	Manager	Employee
Maintain Asset Register	A	R	C	I	I
Maintain Risk Register	A	R	C	I	I
Maintain SSP	I	C	R	I	I
Security	A	C	C	R	R

Awareness					
Incident Response	I	C	R	C	I
Monthly GRC Heartbeat™	A	R	R	C	I
Annual Governance Review	A	R	C	C	I

Legend: R = Responsible | A = Accountable | C = Consulted | I = Informed

Governance Meeting Cadence

Activity	Frequency	Owner
Monthly GRC Heartbeat™	Monthly	Business Owner
Risk Review	Monthly	Executive Sponsor
SSP Review	Quarterly	IT/MSP
Policy Review	Annually	Executive Sponsor
Charter Review	Annually	Executive Sponsor

Small Business Adaptation

In many SMBs, one person performs multiple governance roles. The objective is clear accountability, not organizational complexity.

💡 **Tip:** Document role responsibilities rather than job titles so assignments remain valid as personnel change.

📎 **Related Resources:** F-001 Master Asset Register • F-002 Unified System Security Plan • F-003 GRC Program Charter • G-002 Monthly GRC Heartbeat™ Checklist

Revision History

Version	Date	Author	Description
1.0		Pragmatic GRC™	Initial publication