Resource ID	F-006
Resource Name	Fortify Implementation Guide
Functional Area	Foundation
Related Chapter	Chapter 4
Resource Type	Guide
Format	PDF

Executive Summary

Fortify is the second of the Pragmatic GRC Methodology™'s Four Implementation Guides. It translates security policies into technical safeguards, focusing on identity management, system hardening, vulnerability management, and protecting business systems through repeatable technical practices.

Purpose

To implement and maintain consistent technical security controls — using the Unified System Security Plan as the primary living document.

Guide 2: Fortify

Fortify translates security policies into technical safeguards. It focuses on identity management, system hardening, vulnerability management, and protecting business systems through repeatable technical practices.

Primary Living Document: Unified System Security Plan

Primary Objective: Implement and maintain consistent technical security controls.

Key Tasks Addressed

- Enforcing global Multi-Factor Authentication (MFA) and Single Sign-On (SSO) architectures.

- Executing strict, under-14-day staging and deployment windows for critical security patches.
- Restricting day-to-day user access using the principle of least privilege (giving people access only to what their role actually requires).
- Hardening (closing off unnecessary settings and access points attackers could exploit) local employee endpoints (the laptops, phones, and other devices employees use), production cloud spaces, and virtual networks.

When to Use This Guide

Use Fortify when:

- Implementing new hardware, software, or cloud services.
- Performing routine security maintenance.
- Responding to newly discovered vulnerabilities.
- Preparing for customer security questionnaires or audits.
- Reviewing third-party vendor security.
- Following a significant technology change or system upgrade.

Who Should Participate?

Primary Owner

- IT Manager or Managed Service Provider (MSP)

Supporting Roles

- Business Owner
- Operations Manager
- Department Managers
- Key Technology Vendors (as needed)

Common Mistakes

Avoid:

- Assuming your MSP handles everything without verification.
- Focusing only on technology while ignoring user access.
- Delaying security updates because “nothing has happened.”
- Forgetting to review cloud-based applications and services.

- Implementing security controls that employees routinely bypass.

Success Check

You've successfully completed Fortify when:

- Critical systems are protected using current security controls.
- Administrative access has been reviewed.
- Critical vulnerabilities have assigned remediation plans.
- Backups have been verified.
- Security documentation reflects the current environment.
- Leadership has confidence that the organization's most valuable assets are appropriately protected.