Contents

RAPID Practice Guide (Public)

Rapid Adaptation Process for IT Governance & Deployment

RESCOR LLC Version 11.0 — March 2026

---

1. Introduction

RAPID is a business process for developing, deploying, and maintaining a comprehensive security, governance, risk management, and compliance (SGRC) program. Developed in 1992 and refined through thousands of engagements, RAPID provides a proven framework for managing the continuous changes in business requirements, information technology, the regulatory environment, and the threat landscape.

Origin

RAPID was conceived in 1992 by RESCOR founder Andrew T. Robinson to solve a practical problem: helping nuclear power operators integrate Internet-connected systems into their operations. Nuclear facilities maintain extensive procedure libraries — floor-to-ceiling binders of operational procedures that must be kept current, validated, and accessible. Integrating information security into this environment required breaking the problem into digestible, iterative chunks that could be absorbed without disrupting operations.

This approach — borrowed from Rapid Application Design (RAD) in software engineering — proved applicable far beyond nuclear power. RAPID is, at its core, an agile development process applied to SGRC programs. Just as RAD, Scrum, and DevSecOps break software development into iterative cycles, RAPID breaks SGRC program development into short, focused cycles that produce incremental, measurable improvement.

What RAPID Is

RAPID is an iterative, risk-based architecture process that produces the maximum improvement in an organization's SGRC posture with the least possible time, effort, and cost. RAPID is also a Secure Software Development Lifecycle (SSDLC) — it applies the same iterative, risk-based principles to secure software development that it applies to SGRC programs. RAPID achieves its goals through:

- **Frequent, lightweight development cycles** — analogous to sprints in agile methodology, but driven by real-world triggers rather than fixed time boxes
- **Stakeholder engagement** (historically called "vital perspectives") ensuring buy-in from Board, management, employees, and customers
- **Risk-based prioritization** ensuring the most critical issues are addressed first
- **Continuous validation** through security testing, peer review, and regulatory alignment

What RAPID Is Not

RAPID is not a product, a certification, or a one-time assessment. It is an ongoing process that becomes part of how your organization manages risk. RAPID does not replace your existing risk management framework — it integrates with frameworks such as NIST CSF, NIST 800-37 RMF, ISO 27001, COBIT, COSO, and TOGAF to provide a practical implementation methodology. RAPID is also compatible with other SSDLC methodologies including Scrum, SAFe, and DevSecOps — it can serve as the security governance layer that those methodologies often lack.

Core Principle

A relevant, adaptable, and continuously validated SGRC program is more critical to your business goals than any technology you can buy.

---

2. RAPID Characteristics

Every RAPID-developed program exhibits four essential characteristics:

Relevance

The program is applicable to the organization's business needs, risk tolerance, technological realities, and regulatory environment. A relevant program is specific to the organization — not a generic template.

Rapid Adaptation

The program adapts quickly to changes in business goals, technology, the threat environment, and the regulatory landscape. Adaptation is triggered by real events, not arbitrary schedules.

Continuous Validation

The program is subject to ongoing change management, peer review, security testing, and regulatory alignment. Validation ensures that changes reduce risk while meeting business requirements.

Risk-Based Prioritization

All changes are prioritized by risk level. The most significant exposures are addressed first, ensuring that limited resources produce the greatest reduction in risk.

---

3. RAPID Life Cycle

RAPID consists of four phases. The duration of each phase varies by organization size, complexity, and maturity.

Phase 1: Initiation

The initiation phase establishes the baseline — what exists today, what should exist, and where the gaps are.

Activities: - Collect and analyze existing security program documentation (policies, practices, procedures) - Identify actual practices through interviews with key personnel at all levels - Identify deviations between documented program and actual practices - Perform initial risk assessment using STORM quantitative risk measurement - Organize findings into a RAPID Program Document (RPD) aligned with applicable compliance targets - Identify key stakeholders across all organizational functions - Recommend initial SGRC team composition - Identify initial triggers for SGRC team action

Deliverables: - RAPID Program Document (RPD) — baseline - Risk Assessment Report - Gap Analysis - SGRC team Charter and Composition Recommendation

Duration: 4-12 weeks depending on organizational complexity

Phase 2: Development

The development phase is where the program matures through iterative improvement cycles. RESCOR acts as expert facilitator while the organization builds internal capability.

Activities: - Maintain and update the RPD within the RAPID framework - Facilitate regular SGRC team meetings (every 2-6 months) - Provide expert guidance on risk management, compliance, and security architecture - Make recommendations for program updates based on changes in the business, technology, threat, and regulatory environments - Implement and monitor change management processes - Conduct security testing and risk assessments as scheduled - Train SGRC team members in RAPID processes

Development Cycles: Each cycle follows a **propose-validate-adapt** sequence: 1. Triggers accumulate (security advisories, regulatory changes, business changes, test results) 2. SGRC team convenes to review triggers and propose changes 3. Proposed changes are validated against risk, compliance, and business requirements 4. Validated changes are processed through change management and implemented 5. Change management generates triggers for affected functions

Duration: 4-12 development cycles over 1-3 years. Cycles occur every 2-6 months.

Phase 3: Certification

The certification phase verifies that the program meets all stated control and business objectives.

Activities: - Level-set the security program and risk assessment - Evaluate the program against all applicable control targets and business objectives - Verify that the program is acceptable to auditors, examiners, and regulators - RESCOR certification of program completion

Outcome: A program that demonstrably meets or exceeds all applicable legal, regulatory, and organizational requirements.

Phase 4: Maintenance

The maintenance phase continues for the lifetime of the organization. The organization assumes leadership of the RAPID process; RESCOR transitions to a support role.

Activities: - Organization leads SGRC team meetings and development cycles - RESCOR provides expert consultation as needed - RESCOR reviews and comments on proposed program updates - Security testing and risk assessments continue on schedule - Program adapts to ongoing changes in business, technology, threats, and regulations

Duration: Ongoing — as long as the organization benefits from RESCOR expertise.

---

4. SGRC Teams

The SGRC team is the most important element of RAPID. It is the group of stakeholders empowered to make and implement changes to the organization's security program.

Team Structure

Organizations may have a single SGRC team or multiple teams organized by function (compliance, governance, risk management, security, SSDLC) or by organizational structure (business unit, division, subsidiary). In multi-team structures:

- Each team owns its functional or structural scope
- Changes that affect other teams generate triggers for those teams
- An executive-level steering committee coordinates across teams
- RESCOR facilitates cross-team coordination during development phases

Smaller organizations typically operate with a single team. Larger organizations — especially those with multiple regulatory obligations or complex organizational structures — benefit from specialized teams that coordinate through the RAPID trigger mechanism.

Composition

Each SGRC team must include stakeholders from every organizational function affected by its scope:

- **Board / Executive Leadership** — governance oversight, risk appetite, strategic direction
- **Management** — operational implementation, resource allocation

- **Legal / Compliance** — regulatory requirements, liability, contractual obligations
- **Human Resources** — personnel security, training, termination procedures
- **Information Technology** — technical implementation, system administration
- **Operations / Line of Business** — business requirements, process impact
- **Finance** — budget, cost-benefit analysis, insurance
- **Public Relations / Communications** — incident communication, reputation management

SGRC team Responsibilities

- Maintain security awareness across the organization
- Develop and implement changes to the security program
- Respond to triggers (security incidents, regulatory changes, test results)
- Validate proposed changes against business requirements
- Champion the security program to their respective functions

---

5. RAPID Functional Areas

RAPID organizes security program activities into five functional areas. Every element of the security program falls into one or more of these areas.

Security Awareness

Training and educating all personnel on security policies, practices, and their individual responsibilities. Includes monitoring security advisories, vendor patches, and threat intelligence.

Contingency Management

Responding to security incidents, business disruptions, and disasters. Includes incident response planning, disaster recovery, business continuity, breach notification, and forensic analysis.

Validation

Verifying that the security program is effective through security testing (vulnerability scanning, penetration testing, application testing), configuration analysis, IT audits, peer review, and employee feedback.

Change Management

Prioritizing and implementing changes to the security program. Encompasses policy updates, practice modifications, technical configurations, and procedural changes. Change management generates triggers for affected SGRC teams and functions.

Resource Controls

The technical implementation of the security program. Includes system configurations, access controls, authentication mechanisms, encryption, network architecture, endpoint protection, and all other technical safeguards.

---

6. Scalability Principles

RAPID scales from individual entrepreneurs to the largest enterprises through three principles:

Reduction of Complexity

RAPID divides the target architecture into: - **Functional elements** — security, governance, risk management, compliance - **Structural elements** — organizational hierarchy, business units, functions - **Priority** — criticality-based ordering of activities

Continuous Improvement

Frequent, lightweight development cycles prevent team fatigue, ensure rapid adaptation, maintain focus on critical issues, and provide continuous validation. This is the same principle as Total Quality Management (TQM), ISO 9000, and agile software development.

Stakeholder Engagement

RAPID turns employees into a force multiplier by ensuring that every stakeholder group is represented in the security program development process. Security programs developed without stakeholder buy-in fail — not because they are technically deficient, but because the people who must implement them were not part of the process.

---

7. Framework Integration

RAPID integrates with and supports all major governance, risk, and compliance frameworks:

Risk Management Frameworks

- NIST Cybersecurity Framework (CSF)
- NIST 800-37 Risk Management Framework (RMF)
- NIST 800-30 Risk Assessment
- ISO 31000 Risk Management
- OCTAVE
- FAIR (Factor Analysis of Information Risk)

Governance & Control Frameworks

- ISO 27001 / 27002 Information Security Management
- COBIT (IT Governance)
- COSO (Internal Controls)
- ITIL (IT Service Management)

Architecture Frameworks

- TOGAF (The Open Group Architecture Framework)
- FEAF (Federal Enterprise Architecture Framework)
- DODAF (Department of Defense Architecture Framework)
- Zachman Framework

Compliance Targets

RAPID has been used to achieve and maintain compliance with:

Industry	Regulation / Standard	RAPID Coverage
Financial Services	GLBA (12 CFR Part 364)	Full — all functional areas map to GLBA guidelines
Financial Services	SOX (Sarbanes-Oxley)	IT controls, access management, audit trails
Financial Services	FFIEC Examination Guidelines	Examination preparedness, risk assessment
Financial Services	PCI DSS	Cardholder data protection, access controls
Healthcare	HIPAA Security Rule (45 CFR 164.308)	Full — administrative, physical, technical safeguards
Healthcare	HITECH Act	Breach notification, enhanced enforcement
Healthcare	HITRUST CSF	Comprehensive security framework alignment
Government	FedRAMP	Cloud security authorization
Government	FISMA	Federal information security management
Government	NIST 800-53	Security and privacy controls
Education	FERPA	Student records privacy
Energy	NERC CIP	Bulk electric system cybersecurity
Nuclear	10 CFR 73.54	Nuclear facility cybersecurity
Transportation	TSA Cybersecurity Directives	Pipeline and rail security
General	ISO 27001	Information security management system
General	SOC 2	Service organization controls

---

8. RAPID for Financial Services (GLBA)

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to implement a comprehensive written information security program. The Interagency Guidelines (12 CFR Part 364, Appendix B) specify requirements that map directly to RAPID's functional areas:

Resource Controls (GLBA III.C.1)

- Access controls on customer information systems
- Access restrictions at physical locations containing customer information
- Encryption of electronic customer information in transit and at rest
- Procedures ensuring system modifications are consistent with the security program
- Dual control procedures, segregation of duties, and employee background checks
- Monitoring systems and procedures to detect actual and attempted attacks
- Response programs for unauthorized access to customer information
- Measures to protect against environmental hazards or technological failures

Security Awareness (GLBA III.C.2 & III.E)

- Training staff to implement the institution's information security program
- Board oversight of development, implementation, and maintenance of the program
- Management reporting to the Board at least annually on program status

Validation (GLBA III.C.3)

- Regular testing of key controls, systems, and procedures
- Testing frequency and nature determined by risk assessment
- Independent third-party testing where appropriate

Contingency Management (GLBA III.C.1.g-h)

- Incident response programs for unauthorized access to customer information
- Measures to protect against destruction, loss, or damage due to environmental hazards

RESCOR has served financial institutions ranging from credit unions with less than $10 million in assets to commercial banks with assets exceeding $1.8 trillion.

---

9. RAPID for Healthcare (HIPAA)

The HIPAA Security Rule (45 CFR 164.308) requires covered entities to implement administrative, physical, and technical safeguards for electronic protected health information (ePHI). RAPID's functional areas provide comprehensive coverage:

Resource Controls

- Information access management (164.308(a)(4))
- Personnel security and authorization procedures (164.308(a)(3))
- Physical access controls and facility security (164.310(a))
- Workstation security and device/media controls (164.310(b-d))
- Access controls, audit controls, integrity controls, transmission security (164.312)

Security Awareness (164.308(a)(5))

- Security awareness and training program for all workforce members
- Security reminders, protection from malicious software
- Log-in monitoring and password management training

Validation (164.308(a)(1), (a)(8))

- Risk analysis — accurate and thorough assessment of potential risks to ePHI
- Evaluation — periodic technical and nontechnical evaluation
- Security testing of controls, systems, and procedures

Contingency Management (164.308(a)(7))

- Contingency plan including data backup, disaster recovery, emergency operations
- Testing and revision procedures for contingency plans
- Applications and data criticality analysis

Change Management (164.308(a)(8))

- Hardware and software installation and maintenance review and testing
- Procedures for implementing security updates and patches

---

10. Additional Compliance Coverage

Education (FERPA)

RAPID addresses student records privacy requirements under FERPA (20 USC 1232g) including access controls on education records, directory information opt-out procedures, disclosure logging, and state-specific student data privacy laws.

Transportation (TSA)

RAPID supports TSA Cybersecurity Directives for pipeline, rail, and aviation operators including cybersecurity coordinator designation, CISA incident reporting, vulnerability assessment, and cybersecurity implementation planning for IT and OT environments.

SOC 2 / ISO 27001

RAPID maps to SOC 2 Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy) and ISO 27001:2022 ISMS requirements. Organizations pursuing SOC 2 Type II or ISO 27001 certification can use RAPID as their implementation methodology.

Privacy (CCPA / State Laws)

RAPID addresses the growing patchwork of US state privacy laws (CCPA/CPRA, Colorado CPA, Connecticut CTDPA, Virginia VCDPA, and others) including data inventory and mapping, consumer rights procedures, data protection assessments, and breach notification.

AI Governance

RAPID extends to AI governance requirements under the EU AI Act, NIST AI RMF, Executive Order 14110, and emerging state AI legislation. Coverage includes AI risk assessment, model testing and validation, training data management, human oversight requirements, and vendor AI assessment.

Cloud and Multi-Cloud

RAPID addresses cloud security across AWS, Azure, and GCP including shared responsibility model documentation, IAM, network security, data protection, cloud-specific incident response, infrastructure as code, and multi-cloud coordination.

Supply Chain Risk Management

RAPID incorporates SCRM aligned with NIST 800-161, NIST CSF 2.0, and Executive Order 14028 including vendor risk assessment, software bill of materials (SBOM), ongoing vendor monitoring, concentration risk analysis, and fourth-party risk management.

---

11. RAPID and STORM Integration

RAPID integrates with RESCOR's STORM (Simplified Total Risk Management) quantitative risk measurement to provide:

- **Quantitative risk baselines** at program initiation
- **Measurable progress** from one development cycle to the next
- **Risk-based prioritization** of development cycle activities
- **Comparable measurements** across assessments, organizations, and industries
- **Cost-effectiveness analysis** for proposed controls (STORM "what-if" scenarios)

STORM's entropy-energy model aligns naturally with RAPID's iterative approach: entropy (the natural increase in risk over time) is countered by energy (the investment in RAPID development cycles). STORM makes this dynamic visible and measurable.

---

11. Engagement Model

RAPID is delivered through RESCOR's StrongCOR subscription model:

- **Subscription terms:** 12 to 60 months
- **Flexible service selection:** Choose the services and support that match your organization's needs
- **Adjustable frequency:** Annual, semiannual, quarterly, or monthly service delivery
- **Separation of duties:** RESCOR cannot support a system it is hired to test, ensuring assessment objectivity

For more information, contact RESCOR at +1 863 SECURE1 (+1 863 732-8731) or visit www.rescor.net/contact/.