The Gridiron Compliance Model

aptible

Aptible Gridiron helps software engineering teams easily stand up and maintain information security management programs that can meet stringent compliance and security requirements, such as HIPAA, SOC 2, or ISO 27001. Gridiron's toolset breaks down complex frameworks into clear business processes, and gives you powerful tools to reduce risk and save time.

Risk Analysis

Initial tasks:

- Develop risk model
- Analyze threats
- Select security controls
- Approve an operational risk profile

Ongoing tasks:

- Update risk and threat models as new information becomes available, operational circumstances change
- Monitor and assess security controls
- Re-assess and re-approve risk profile

Incident Response

Initial tasks:

- Develop incident response capabilities (alerting, notification chain, training, testing)
- Develop business continuity plans and capabilities
- Ensure response capabilities support business and legal requirements (SLAs, breach reporting)

Ongoing tasks:

- Test response capabilities
- Respond to incidents
- Track incident response metrics
- Improve based on retrospectives

Policies and Procedures

Initial tasks:

- Use risk analysis results to select reasonable and appropriate administrative controls
- Ensure control program meets legal and regulatory requirements
- Ensure policies and operating procedures support business goals

Ongoing tasks:

- Update and re-approve policies as risk profile changes
- Audit (internal or external) compliance with policies, procedures, and standards

Operations

Initial tasks:

- Implement security controls (administrative/physical/technical)

Strong compliance programs maximize time spent on core operations.

Ongoing tasks:

- **Focus on your business**
- Develop and maintain secure applications
- Review access controls and logs
- Track security milestones and metrics
- Manage vendor risk
- Identify potential incidents

Security and Privacy Training

Initial tasks:

- Train workforce members based on roles and access to sensitive data
- Train workforce members on how to protect sensitive data
- Advanced secure development training for software engineers and designers

Ongoing tasks:

- Update training content
- All workforce members must re-certify