Action1
#1 for patch management

Patch Management Compliance Guide

In a landscape of evolving regulations and increasingly intricate and dispersed IT environments, maintaining continuous patch compliance proves to be a challenge for IT teams. In the pursuit of compliance, having accurate information about requirements and effective strategies is essential. This guide consolidates patch requirements* from key compliance frameworks: PCI DSS, HIPAA, SOC 2, CIS CSC, ACSC Essential Eight, GLBA/FFIEC.

PCI DSS (Payment Card Industry Data Security Standard)

- Deploy critical security patches within a month of release
- Establish a process to identify new security vulnerabilities
- Use reputable sources to receive vulnerability information
- Evaluate relevant vulnerabilities to assess risk
- Develop a plan for addressing vulnerabilities
- Prioritize patches based on risk level
- Regularly test security patches in a non-production environment
- Apply patches to production systems within a reasonable timeframe
- Maintain documentation of patch management processes and procedures

HIPAA (Health Insurance Portability and Accountability Act)

- Implement policies and procedures to address the application of security patches
- Regularly assess software vulnerabilities and potential risks
- Develop a strategy to address security vulnerabilities that may pose a risk to electronic protected health information (ePHI)
- Apply security patches to address identified vulnerabilities in a timely manner
- Consider security patches as part of the overall risk management process
- Implement mechanisms to detect and report security incidents and vulnerabilities
- Monitor security news sources and stay informed about emerging security threats and vulnerabilities
- Establish a process for evaluating and testing security patches before deployment
- Document patch management processes and procedures for future reference and auditing

SOC 2 (System and Organization Controls 2)

- Establish a formal patch management policy and procedures
- Regularly assess software vulnerabilities and threats
- Prioritize vulnerabilities based on risk assessment
- Develop a plan to address identified vulnerabilities promptly
- Test patches in a controlled environment before deployment
- Implement a process to monitor patch status across systems
- Maintain documentation of patch management activities and outcomes
- Monitor industry sources for information about new vulnerabilities
- Implement security controls to prevent unauthorized access to systems
- Review and update the patch management policy periodically
- Integrate patch management into the broader risk management framework

CIS CSC (Center for Internet Security Critical Security Controls)

- Maintain an inventory of hardware and software assets
- Establish a formalized patch management policy and procedures
- Regularly assess software and system vulnerabilities
- Prioritize vulnerabilities based on potential impact and exploitability
- Develop a process to test and evaluate patches in a controlled environment
- Apply patches to systems and software within a reasonable timeframe
- Monitor and verify that patches are effectively deployed
- Automate patch management processes wherever possible
- Maintain a backup and rollback plan in case patches cause issues
- Continuously monitor security news and sources for emerging threats
- Document patch management activities and outcomes for auditing
- Integrate patch management into the overall cybersecurity strategy

Australian Cyber Security Centre (ACSC) Essential Eight

- Establish a formal patch management policy and procedures
- Regularly identify and assess vulnerabilities within systems and applications
- Prioritize vulnerabilities based on risk and potential impact
- Develop a plan to apply patches in a timely and effective manner
- Test patches in a controlled environment before deploying them to production systems
- Maintain documentation of patch management activities and decisions
- Implement automated mechanisms for patch deployment where feasible

- Monitor and track the status of patches across systems
- Stay informed about emerging vulnerabilities and threats through reliable sources
- Integrate patch management into the broader cybersecurity strategy
- Review and update the patch management process periodically

Gramm-Leach-Bliley Act (GLBA) and the Federal Financial Institutions Examination Council (FFIEC)

- Establish a formal patch management policy and procedures
- Regularly assess vulnerabilities in systems and applications
- Prioritize vulnerabilities based on risk and potential impact on sensitive financial data
- Develop a plan to apply patches promptly and efficiently
- Test patches in a controlled environment before deployment
- Monitor and verify the successful deployment of patches
- Document patch management activities and decisions for auditing
- Implement a process to stay informed about security updates and vulnerabilities
- Integrate patch management into the overall risk management framework
- Collaborate with third-party vendors to ensure the security of software and systems
- Review and update the patch management process regularly to address evolving threats

Continuous Patch Compliance with Action1

Automate some of the most tedious patch compliance activities to reduce risk to your environment and data, pass compliance audits faster and with a better compliance rate, and free up your time for other strategically important IT projects. Explore what patch compliance activities you can streamline with Action1, the first vendor focusing on patch management to achieve both ISO 27001:2022 and SOC 2 Type II:

- Discover, prioritize and remediate vulnerabilities
- Ensure continuous patch compliance for servers and workstations
- Automate patch management for OS and third-party apps
- Maintain up-to-date inventory
- Enforce secure endpoint configurations
- Setup patch compliance reporting
- Apply policy-based patching
- Schedule patch deployments flexibly

*Please note that these are general considerations based on PCI DSS, HIPAA, SOC 2, CIS CSC, ACSC Essential Eight, GLBA/FFIEC guidelines. Always refer to the official documentation for precise and current guidance specific to your institution's compliance requirements.