sonatype

Meet ISM Software Development Guidelines with Sonatype

User’s Guide to Compliance

In March 2024, the Australian Signals Directorate published the latest update to its Information Security Manual (ISM). The ISM provides a framework based on risk management principles and best practices to help CISOs, CIOs, cyber security professionals, and IT managers protect their systems and data from cyber threats.

The ISM includes cyber security guidelines designed to 'provide practical guidance on how an organisation can protect its systems and data from cyber threats.' These include Guidelines for Software Development, which provide a useful set of guidelines for creating traditional and mobile applications to increase security. The ISM is a framework, so organisations are not yet required by law to comply. However, it's a useful tool for companies to ensure they do not violate existing legislation, and under its guidance, organisations can put up a pretty effective defence against data breaches.

We explore how Sonatype can help meet the requirements of the ISM controls

Sonatype has been at the forefront of helping organisations defend themselves from security risks, and in this document, **we explore how Sonatype can help meet the requirements of the ISM controls** outlined in its Guidelines for Software Development.

ISM Control Requirement	Sonatype Capability
DEVELOPMENT, TESTING, AND PRODUCTION ENVIRONMENTS *Segregating development, testing and production environments, and associated data, can limit the spread of malicious code and minimises the likelihood of faulty code being introduced into a production environment. Furthermore, protecting the authoritative source for software is critical to preventing malicious code being surreptitiously introduced into software.*	
ISM-0400 Development, testing, and production environments are segregated.	**Sonatype Nexus Repository** Provides controlled and separate repositories for each stage to ensure the segregation of development, testing, and production environments.
ISM-1419 Development and modification of software only take place in development environments.	**Sonatype Nexus Repository** Ensures the development and modification of software occurs only in development environments through the management of access controls and repository permissions.
ISM-1422 Unauthorised access to the authoritative source for software is prevented.	**Sonatype Nexus Repository | Sonatype Repository Firewall | Sonatype Lifecycle** Prevents unauthorised access to the authoritative source for software by implementing robust access controls and audit logging. Implementing Repository and Firewall ensures that only authorised sources are allowed to be in your software development environments.

ISM-1816 Unauthorised modification of the authoritative source for software is prevented.	**Sonatype Nexus Repository | Sonatype Repository Firewall** Prevents unauthorised modification of the authoritative source for software by scanning for and blocking malicious components. Sonatype Repository is used to store authoritative versions of software releases.

SECURE SOFTWARE DESIGN AND DEVELOPMENT

The use of secure-by-design and secure-by-default principles, memory-safe programming languages (such as C#, Go, Java, Ruby, Rust and Swift), and secure programming practices that are supported by agile software development practices and threat modelling are an important part of application development as they can assist with the identification and mitigation of at risk software components and risky programming practices. In addition, providing mechanisms to assist in determining the authenticity and integrity of applications, while configuring them in a secure manner, can assist with software supply chain security activities.

ISM-0401 Secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices are used as part of application development.	**Sonatype Lifecycle** Promotes secure-by-design and secure-by-default principles and the use of secure programming practices by identifying and managing security risks in open source components.
ISM-1780 SecDevOps practices are used for application development	**Sonatype Lifecycle** Supports SecDevOps practices by integrating security into the software development lifecycle and providing continuous monitoring and feedback.
ISM-1238 Threat modelling is used in support of application development.	**Sonatype Lifecycle** Facilitates threat modelling by providing visibility into open source component usage and associated vulnerabilities, enabling proactive risk management.
ISM-1796 Files containing executable content are digitally signed as part of application development.	**Sonatype Nexus Repository** Ensures files containing executable content are digitally signed by managing and storing signed artifacts.
ISM-1797 Installers, patches, and updates are digitally signed or provided with cryptographic checksums as part of application development.	**Sonatype Nexus Repository** Manages and verifies signatures to ensure installers, patches, and updates are digitally signed or provided with cryptographic checksums.
ISM-1798 Secure configuration guidance is produced as part of application development.	**Sonatype Lifecycle** Produces secure configuration guidance by analysing components and providing best practices for secure configuration.

A SOFTWARE BILL OF MATERIALS (SBOM)

A software bill of materials is a list of open source and commercial software components used in application development. This can assist in providing greater cyber supply chain transparency for consumers by allowing for easier identification and management of security risks associated with individual software components used by applications.

ISM-1730
A software bill of materials (SBOM) is produced and made available to consumers of software.

Sonatype Lifecycle | Sonatype SBOM Manager
Produces SBOMs and makes them available to consumers, enhancing supply chain transparency and security.

APPLICATION SECURITY TESTING

Application security testing can assist software developers in identifying vulnerabilities in their applications. In doing so, both static application security testing, as well as dynamic application security testing, should be performed in order to achieve comprehensive test coverage. Furthermore, software developers may choose to use an additional independent party to assist with removing any potential for bias that might occur when they test their own applications.

ISM-0402
Applications are comprehensively tested for vulnerabilities, using both static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.

Sonatype Lifecycle | Sonatype Developer
Supports comprehensive application security testing by integrating with SAST and DAST tools to identify vulnerabilities before release. ***Note: Sonatype will soon have SAST included with Sonatype Developer***

VULNERABILITY DISCLOSURE PROGRAM

Implementing a vulnerability disclosure program, based on responsible disclosure, can assist an organisation to improve the security of their products and services as it provides a way for security researchers and other members of the public to responsibly notify them of vulnerabilities in a coordinated manner. Furthermore, following the verification and resolution of reported vulnerabilities, it can assist an organisation in notifying their customers of vulnerabilities that have been discovered in their products and services, and any patches, updates or vendor mitigations that should be applied.

ISM-1616
A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.

Sonatype Lifecycle | Sonatype Nexus Repository Sonatype Repository Firewall | Sonatype SBOM Manager
Implements a vulnerability disclosure program by providing tools to manage and track vulnerabilities reported by internal and external parties.

ISM-1755
A vulnerability disclosure policy is developed, implemented and maintained.

Sonatype Lifecycle | Sonatype Nexus Repository Sonatype Repository Firewall | Sonatype SBOM Manager
Supports the development, implementation, and maintenance of a vulnerability disclosure policy by tracking and managing reported vulnerabilities.

ISM-1756 Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed, implemented and maintained.	**Sonatype Lifecycle | Sonatype Nexus Repository Sonatype Repository Firewall | Sonatype SBOM Manager** Develops, implements, and maintains vulnerability disclosure processes and procedures by providing a centralised platform for vulnerability management.
REPORTING AND RESOLVING VULNERABILITIES *Following the identification of vulnerabilities, either via internal application security testing or external security researchers, software developers should ensure that such vulnerabilities are reported and resolved in a timely manner. In doing so, software developers should perform root cause analysis and, to the greatest extent possible, seek to remediate entire vulnerability classes.* *If vulnerabilities cannot be resolved by software developers in a timely manner via patches or updates, software developers should provide advice on how, to the greatest extent possible, the likelihood of vulnerabilities being exploited can be reduced, the impact of vulnerabilities being exploited can be reduced or both.*	
ISM-1908 Vulnerabilities identified in applications are publicly disclosed (where appropriate to do so) by software developers in a timely manner.	**Sonatype Lifecycle | Sonatype Nexus Repository | Sonatype Repository Firewall** Publicly discloses vulnerabilities identified in applications in a timely manner by providing tools to track and manage the disclosure process.
ISM-1754 Vulnerabilities identified in applications are resolved by software developers in a timely manner.	**Sonatype Lifecycle | Sonatype Nexus Repository | Sonatype Repository Firewall** Resolves application vulnerabilities in a timely manner by integrating with development workflows to prioritise and address security issues.
ISM-1909 In resolving vulnerabilities, software developers perform root cause analysis and, to the greatest extent possible, seek to remediate entire vulnerability classes.	**Sonatype Lifecycle | Sonatype Nexus Repository | Sonatype Repository Firewall** Performs root cause analysis and seeks to remediate entire vulnerability classes by providing insights into vulnerability trends and patterns.

These updates to ISM reflect a broader global trend towards more comprehensive – and consequential – data protection regulations and highlight the importance of implementing robust privacy and security measures. Now is the time to evaluate your defences. If you're interested in speaking with a Sonatype expert about what to do next, **we'd love to hear from you**.

sonatype

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Life Cycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com