MAPPING GUIDE

Imprivata FairWarning Mapping to ISO/IEC 27001

Background on the ISO/IEC 27001:2013 Standard

ISO/IEC 27001:2013 is an international standard that describes best practices for an information security management system (ISMS). As defined by the ISO organization, the ISO standards "will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties." https://www.iso.org/isoiec-27001-information-security.html

It is commonly known as ISO 27001 (ISO = Intranational Organization for Standardization).

The ISO organization is based in Geneva, Switzerland. The most recent version of the ISO 27001 standard was published in September 2013.

Purpose of an Information Security Management System

An information security management system (ISMS) is a set of frameworks that contain policies and procedures for tackling security risks in an organization. The focus of an ISMS is to ensure business continuity by minimizing all security risks to information assets and limiting security breach impacts to a bare minimum.

The ISO 27001 standard describes how an ISMS can be built at an organization. Through implementation, it requires the organization to develop a set of information security rules, responsibilities, and controls, which then enable the organization to manage its complex systems and the security risk that arises from them.

Other ISO Standards

In addition to ISO 27001, there is the ISO 27002 standard. Whereas the ISO 27001 standards states and defines the audit requirements, ISO 27002 provides best practice recommendations on the implementation of information security management by those who are responsible for implementing or maintaining the ISMS. As the ISO Organization states, the ISO 27002 is a "code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001". ISO 27002 recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity, and availability of information.

The items in ISO 27002 are the same as items in ISO 27001's Annex A. Each control from Annex A exists in ISO 27002, together with a more detailed explanation of how to implement it.

Addressing ISO 27001 through use of Imprivata FairWarning

For clarity in showing how Imprivata FairWarning's capabilities assist in ISO 27001 implementation and support, the items in Annex A are presented below.

The annex is not required of organizations implementing ISO 27001. This means that certified organizations are expected to use it, but they are free to deviate from or supplement it to address their specific information risks.

ISO 27001's Annex A contains the groups, objectives, and controls associated with the standard. Specifically, there are now 114 controls in 14 groups and 35 control objectives within the 2013 version.

Note that this document contains only a subsection of the Annex A items that are supported (in full or partially) by Imprivata FairWarning's Patient Privacy Intelligence (PPI) and Managed Privacy Services (MPS) capabilities.

* A.5: Information security policies
* A.6: Organization of information security
* A.7: Human resource security
* A.8: Asset management
* A.9: Access control

  A.10: Cryptography

  A.11: Physical and environmental security *A.12: Operations security

  A.13: Communications security
* A.14: System acquisition, development and maintenance
* A.15: Supplier relationships
* A.16: Information security incident management

  A.17: Information security aspects of business continuity management
* A.18: Compliance (with internal requirements, such as policies, and with external requirements, such as laws)

In this report of Imprivata FairWarning's applicability and full or partial support of ISO 27001, we focus on 40 controls that are within the groups starred above.

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.5 Information security policies **A.5.1 Management direction for information security** Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	As part of the onboarding process with Imprivata FairWarning, customers determine and deploy alerts that monitor access rights management. These Imprivata FairWarning alerts assist the customer in the development and encirclement of their organization's privacy and security policies.	Full
A.6 Organization of information security **A.6.1 Internal organization** Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.				
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Customer uses workflows for incident response management within the Imprivata FairWarning application. These incidents assist the customer in defining incidents and assigning applicable staff to remediate.	Full
A.7 Human resource security **A.7.2 During employment** Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.				
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Imprivata FairWarning assists customers in two ways with this control. First, the customer can gain insight into data access and usage of its account holders. This helps them ensure their privacy and security policies and procedures are being met. Secondly, Imprivata FairWarning provides educational material to customers. These materials assist managers in setting expectations with their staff about what will be monitored via Imprivata FairWarning. This education and monitoring assist in moving customer culture towards optimal compliance and security practices.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Imprivata FairWarning provides incident response tracking and management through forensically sound data. If incident is determined by customer to be due to an employee security breach, information provided by Imprivata FairWarning may be used in a disciplinary process.	Full
A.8 Asset management **A.8.1 Responsibility for assets** Objective: To identify organizational assets and define appropriate protection responsibilities.				
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Customers use the Imprivata FairWarning application to monitor access to confidential information such as PHI, PII, and/or intellectual property. This monitoring assists customers in both 1) identifying and documenting violations of appropriate access to confidential data and 2) implementing security controls to enforce appropriate access. This monitoring and any associated remediation of inappropriate access helps ensure acceptable use of the confidential information.	Full
A.8.2 Information classification Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.				
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	As part of its onboarding process with Imprivata FairWarning, the customer prioritizes information in highest need of user access monitoring. The customer may prioritize information because the criticality of the applications, legal requirements or other values.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.9 Access control				
A.9.1 Business requirements of access control				
Objective: To limit access to information and information processing facilities.				
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Imprivata FairWarning assists customers, through the use of behavioral analytics, in the detection of access violations as specified by the customer's policies. This provides customers insight into what their users are accessing. With this information, customers may craft access control policies that meet their business and security requirements.	Full
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Customer may use Imprivata FairWarning's platform to gain visibility into the data access patterns of their users. Based on that information, customers can remediate access violations and ensure authorized access and use.	Full
A.9.2 User access management				
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.				
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Imprivata FairWarning assists its customers in regularly monitoring what information their users are accessing. The Imprivata FairWarning platform can aid in determining who is currently accessing what (documenting) and provide evidence to support establishing and changing access control policies.	Full
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Customers may use Imprivata FairWarning to monitor if terminated employees are accessing data. This alerting can help customers identify any gaps in their employee deprovisioning process that allow for continued access after termination.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.9.4 System and application access control Objective: To prevent unauthorized access to systems and applications.				
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Imprivata FairWarning assists its customers to regularly monitor what information their users are accessing. The Imprivata FairWarning platform can aid in determining who is currently accessing what, documenting and providing evidence to support establishing and changing of access control policies.	Partial
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Imprivata FairWarning can provide customers information on how, when, from where, etc. users are logging into systems. This data assists customers in identifying if secure logon procedures are met.	Partial
A.12 Operations security **A.12.2 Protection from malware** Objective: To ensure that information and information processing facilities are protected against malware.				
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Imprivata FairWarning application helps customers detect potential security violations and provides incident tracking and management. This allows for full documentation of post-incident analysis, resolution, mitigation, and other activities. Imprivata FairWarning can detect file manipulation, compromised account credentials, and other changes which may be indicative of malware infection.	Partial
A.12.3 Backup Objective: To protect against loss of data.				
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	For its SaaS customers, Imprivata FairWarning maintains backup copies of audit files for monitored data sources. Restoration of these backup files is tested regularly.	Partial

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.12.4 Logging and monitoring Objective: To record events and generate evidence.				
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Through their use of the Imprivata FairWarning platform, a customer may keep and regularly review the event logs of monitored data sources.	Full
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Through ongoing health check monitoring, Imprivata FairWarning ensures the integrity and confidentiality of audit logs it receives from customers.	Partial
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	A customer may use the Imprivata FairWarning platform to log and regularly review the access patterns of its administrators and operators.	Full
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Imprivata FairWarning synchronizes data logs it receives from customers to a single reference time source.	Full
A.12.5 Control of operational software Objective: To ensure the integrity of operational systems.				
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Imprivata FairWarning provides information to customers on the installation of software on select monitored data sources. Customers may use this information to implement controls to block these installations.	Partial
A.12.7 Information systems audit considerations Objective: To minimise the impact of audit activities on operational systems.				
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Imprivata FairWarning's platform and audit extraction processes are planned and implemented to minimize any disruptions to customers and their business processes.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.14 System acquisition, development and maintenance				
A.14.1 Security requirements of information systems				
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.				
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	When obtaining data from customers over public networks, Imprivata FairWarning employs secure protocols and dedicated communication channels. These practices protect transmitted information integrity and confidentiality.	Full
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	When obtaining data from customers over public networks, Imprivata FairWarning employs secure protocols and dedicated communication channels. These practices protect transmitted information integrity and confidentiality.	Full
A.14.2 Security in development and support processes				
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.				
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Any updates to the Imprivata FairWarning application go through a formal change control process internally. Customers are kept updated on these changes and may elect to use their own change control procedures for changes to their production of Imprivata FairWarning applications.	Full
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	All updates to the Imprivata FairWarning application go through an extensive quality assurance process before being made available to customers.	Full
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Imprivata FairWarning provides information to customers on the installation of software on select monitored data sources. Customers may use this information to implement controls for these changes.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Proper controls are in place in regards to product engineering of the Imprivata FairWarning application, including separation of duties, quality assurance checks and change control.	Full
A.15 Supplier relationships **A.15.2 Supplier service delivery management** Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.				
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Imprivata FairWarning provides analytics and alerts about access in systems with confidential data. These analytics and alerts include monitoring, reviewing and auditing activity from third parties such as suppliers.	Full
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Imprivata FairWarning provides analytics and alerts about access in systems with confidential data. These analytics and alerts include monitoring, reviewing and auditing activity from third parties such as suppliers.	Full
A.16 Information security incident management **A.16.1 Management of information security incidents and improvements** Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt and orderly documentation of post-incident analysis, resolution mitigation and other activities.	Full
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt and appropriate reporting of security incidents and their management.	Full
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt detection and reporting of any security weaknesses in the areas of user access management and auditing.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Imprivata FairWarning's platform provides incident response detection and insight into what caused the incident (i.e., compromised login credentials, elevation of access privileges, etc.). With this information, customers are able to better understand incidents and classify them appropriately.	Full
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in assessing how effective (or ineffective) their procedures are and if they align with documented procedures.	Full
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Imprivata FairWarning's platform provides incident response detection and insight into what caused the incident (i.e., compromised login credentials, elevation of access privileges, etc.). With this information, customers are able to better understand incidents, identify the risks that facilitated the incident, and implement security controls as needed.	Full
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Imprivata FairWarning's platform provides incident response tracking and management through forensically sound data. In addition, it provides incident response tracking and management via the investigation section allowing for full documentation of post incident analysis, mitigation, and resolution. Customers can use the platform's capabilities to define and implement procedures that enable information to become evidence.	Full
A.18. Compliance **A.18.1 Compliance with legal and contractual requirements** Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.				
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Through the use of Imprivata FairWarning's monitoring and alerting, in the areas of user access and auditing, a customer can assess its ongoing compliance. Compliance to protect the customer's IP and proprietary products may be due to legislation, regulations and/or contractual requirements.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	Imprivata FairWarning's platform enables its customers to monitor confidential data and detect if unauthorized changes, access, release or loss are made to this data. The customer then can apply security controls and protections as needed and demonstrate compliance.	Full
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Imprivata FairWarning's platform enables its customers to monitor access in systems with confidential data and alert if this access violates security and privacy controls. Because of this, a customer can ensure that the privacy of its PII is maintained and only accessed by those with legitimate need to know.	Full
A.18.2 Information security reviews Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.				
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Through Imprivata FairWarning's ongoing monitoring and alerting to what confidential data users are accessing, a customer gains insight into the efficacy of their access control policies and processes. This insight can assist the customer in their security efforts related to user access.	Full
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Through the use of Imprivata FairWarning's monitoring and alerting, a customer can assess its ongoing compliance to standards, like HIPAA, in the areas of user access management and auditing.	Full
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Through the use of Imprivata FairWarning's monitoring and alerting, a customer can assess its ongoing compliance to its own internal policies and standards in the areas of user access management and auditing.	Full

*The data above represents a subset of the ISO controls. It only lists those controls where Imprivata FairWarning has full or partial capability to help customers satisfy this control.