How OneTrust Helps: Information Security

DECEMBER 5, 2018

WHITE PAPER

OneTrust
Privacy Management Software

Table of Contents

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

Introduction

With the EU General Data Protection Regulation (GDPR) now in force, and other new privacy laws on its heels, the concept of “adequate security” is becoming a legal mandate on a global level, and it is now commonly understood that privacy cannot truly be done without security. This overlap between privacy and security calls for new ways for these two teams to collaborate, communicate more effectively, and use common tools.

OneTrust helps with the establishment, maintenance and continual improvement of an information security management system (ISMS), as well as the planning and implementation of industry standards such as ISO 27001, AICPA TSC (SOC 2), CSA STAR, NIST CSF and more.

What is an ISMS?

An ISMS is an organization’s systematic approach to managing and protecting the confidentiality, integrity and availability (CIA) of information. More specifically, an ISMS includes the policies, procedures, guidelines, resources, activities and controls employed in pursuit of that aim.

So, if the goal of a privacy team is to implement Privacy by Design—the proactive embedding of privacy into the design specifications of information technologies, network infrastructure and business practices—then the goal of an ISMS team would be to accomplish that very same thing, but with security—i.e., to implement “Security by Design.”

Naturally then, an effective ISMS necessitates skilled decision-making, documented policies and procedures, awareness training, clear lines of responsibility and asset ownership, risk assessments and risk treatment plans, incident response, vendor management, internal auditing, and more.

Security Under the GDPR

Security of processing is a foundational principle of the GDPR. Under Article 5(1)(f), personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

This principle is further incorporated in Article 32, which mandates the implementation of "appropriate technical and organisational measures to ensure a level of security appropriate to the risk." It is this "appropriateness" that is so important, as it is clear that because the GDPR takes a risk-based approach, an organization's security does not have to be perfect and there is also no one-size-fits-all solution. This provides a great deal of flexibility for organizations in forming their information security program, as it often calls for a risk-assessment and risk-treatment process that is inherently subjective in nature. However, this can also lead to a high level of uncertainty for organizations trying to do the right thing.

EU Supervisory Authority Guidance

Fortunately, a number of regulatory authorities and standards bodies have provided guidance on what it means to have "appropriate" security.

UK Information Commissioner's Office (ICO)

For example, the UK ICO has provided a checklist[1] for controllers and processors to use to assess security in their organizations, along with guidance on what needs to be protected, the level of security that is required, the measures that need to be considered, what to do if operating in a sector that has its own security requirements, and more. The ICO also recommends the "Cyber Essentials"[2] baseline set of controls—firewalls, secure device settings, access controls, anti-malware, and software updates—as a "good starting point" and then building a program out from there depending on the organization's particular circumstances and risks.

French Commission nationale de l'informatique et des libertés (CNIL)

France's supervisory authority, the CNIL, has also published a guide to securing personal data, in which they place particular emphasis on the risk-based approach discussed earlier:

> *Such an approach allows for objective decision-making and the determination of the measures strictly necessary and suitable to the context. It is, however, often difficult, when you are not familiar with these methods, to apply such an approach to ensure that the required measures have indeed been implemented.*

[1] UK ICO Guide to the GDPR, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

[2] NCSC Cyber Essentials, https://www.cyberessentials.ncsc.gov.uk/

The CNIL guide then proceeds to list "the basic precautions which should be implemented systematically" in a risk management context that includes the following four stages:

1. listing the processing of personal data, the data processed, and the media on which they rely;

2. assessing the risks generated by each processing operation;

3. implementing and checking the planned measures; and

4. carrying out periodical security audits, with each audit producing an action plan "monitored at the highest level of the organisation."

The CNIL even goes on to state that this process "could help to fill in the section on the risk assessment of the [DPIA]" and that "[i]nformation security risk management can be carried out at the same time as privacy risk management since these approaches are compatible"—an excellent point if we do say so **ourselves**.

Having a strong information security program can also be viewed as a mitigating factor for a supervisory authority calculating a potential fine. For example, under Article 83(2) of the GDPR, "the intentional or negligent character of the infringement" as well as "the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them" are just two mitigating factors that a supervisory authority must take into account when deciding on an administrative fine. In other words, being able to show that you have an established information security program with industry standard measures, as opposed to being asleep at the wheel, should hopefully go a long way in the eyes of a **supervisory authority**.

Security Frameworks

In addition to regulatory guidance, there are also a number of pre-existing information security frameworks that can be leveraged.

For instance, the IAPP and OneTrust published a whitepaper together identifying six main areas of common ground between the ISO 27001 standard and the GDPR, "intended to demonstrate how ISO 27001-certified organizations are well positioned to respond to many GDPR priorities."

Although they come from different perspectives, ISO 27001 and the GDPR at their core are both about reducing risk to people and organizations caused by misuse of personal data, with demonstrable overlap in both principles and requirements.

Additionally, there is significant overlap with the AICPA Trust Service Criteria (TSC),[3] which serves as the basis for the popular SOC 2 report, as well as with the Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR),[4] the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF),[5] and more. Moreover, many of these frameworks, and others like them, have been mapped to one another to reveal their many areas of overlap (e.g., as seen in the CSA CAIQ[6]).

These frameworks are well respected, having served as industry standards for many years and can be immensely valuable as part of establishing your overall security posture.

What is ISO 27001?

ISO 27001[7] is an international standard, developed by the International Organization for Standardization (ISO), that describes how to establish, maintain and continually improve an ISMS. ISO 27001 is one of the most popular and commonly used information security standards, and countless organizations have certified against it for the purpose of demonstrating adequate security to customers, business partners and regulators. The latest revision of the ISO 27001 standard was published in 2013 (ISO/IEC 27001:2013).

Organizations that meet the requirements of ISO 27001 can be certified by an accredited certification body after successfully completing an audit against the standard. According to the ISO, over 39,000 organizations held certification in 2017.[8]

ISO 27001 takes a holistic approach to information security, including the development of clear and comprehensive policies and procedures that take organizational context and scope into account, the appointment of leadership roles with defined responsibilities, ongoing security training and awareness, and more.

How OneTrust Helps with Information Security

The following will use ISO 27001 as a case study for demonstrating how OneTrust helps with information security management, relating specifically to:

- Documentation
- Security Awareness Training, Testing and Attestation
- Risk Assessment and Treatment
- Statement of Applicability
- Internal Audits
- Asset and Vendor Inventory
- Incidents and Breaches

[3] AICPA Trust Services Criteria, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[4] CSA Star, https://cloudsecurityalliance.org/star/#_overview

[5] NIST CSF, https://www.nist.gov/cyberframework

[6] CSA CAIQ, https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1

[7] ISO 27001, https://www.iso.org/isoiec-27001-information-security.html

[8] ISO Survey, https://www.iso.org/the-iso-survey.html

ISMS Decision-Making

ISO 27001 provides a roadmap for building a comprehensive ISMS and implementing only those security controls that make sense for the organization based on a risk assessment. This roadmap includes determining both the internal and external issues that might affect security (including taking the interests of third parties into account) to determine scope and context, and then creating policies and procedures to match.

Specifically, Clause 4 of ISO 27001 requires that you document the internal and external factors affecting your ISMS, as well as the needs and expectations (including requirements) of any interested parties that are relevant to the ISMS, and that you take these things into account when determining the scope (i.e., the boundaries and applicability) of your ISMS. Finally, Clause 4 requires that the ISMS be formally documented and undergo continuous improvement.

Clause 5 is concerned with leadership and responsibilities—ensuring an organization-wide commitment to information security, communicating a documented information security policy throughout the organization, and having defined roles and responsibilities with respect to information security.

Clause 6 is about planning—including creating a documented procedure for identifying, assessing and treating information security risks and opportunities for improvement, as well as a process for identifying information security objectives and creating detailed plans on how to achieve them. Risk treatment plans and ISMS objectives should be "S.M.A.R.T."—Specific, Measurable, Achievable, Relevant, and Time bound. Finally, Clause 6 requires you to create a "statement of applicability" that documents the ISO/IEC 27001:2013 Annex A controls that have deemed applicable to the ISMS.

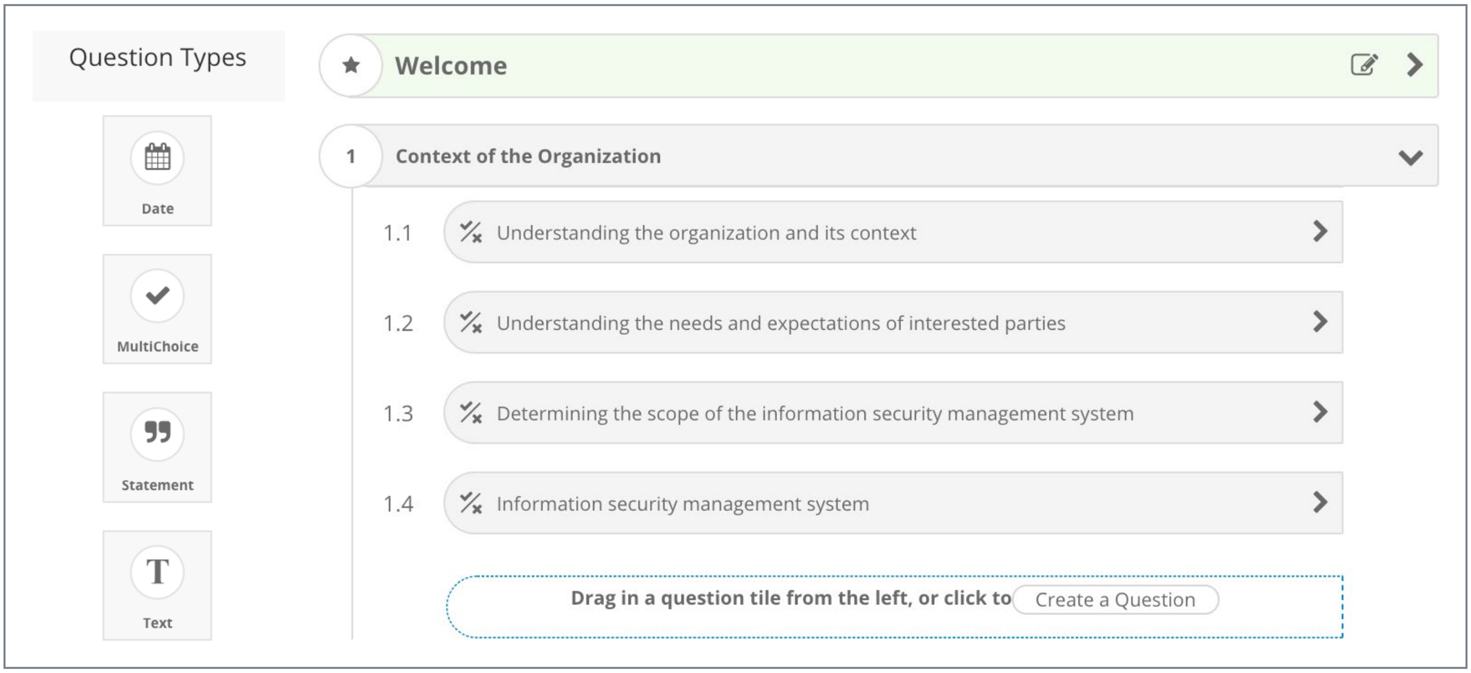
Clause 7 is about support for the ISMS. It requires that you allocate the resources necessary for achieving your objectives and to ensure continuous improvement of your ISMS, as well as ensuring that in-scope personnel have the necessary levels of information security education, training and experience. It also requires that you ensure organization-wide awareness of information security policies and procedures, and individual roles and responsibilities with respect to security (e.g., that information security is the responsibility of all personnel). Lastly, Clause 7 requires a documented policy and procedure for handling both internal and external communications about the ISMS, as well as a documented policy and procedure for ensuring the proper review and approval of new or updated ISMS documentation, as well as for proper control and handling of documentation.

Clause 8 is primarily about implementation of the plans set out in Clause 6. It requires that you undergo risk assessments at planned intervals or when significant changes are planned or occur, and that you document the results. It subsequently requires you to create and carry out risk treatment plans following the risk assessment, and to document the results of treatment.

Clause 9 requires that you conduct internal audits of the ISMS against the ISO/IEC 27001:2013 standard (including Clauses 4-10 and applicable Annex A controls), and that you conduct management reviews of the ISMS at planned intervals.

Lastly, Clause 10 calls for a documented corrective action procedure for addressing 'nonconformities' with the ISO/IEC 27001:2013 standard. Nonconformities are typically identified during audits. Nonconformities identified during an external certification or surveillance audit are usually accompanied by deadlines for completing corrective actions, and in some cases a failure to correct a nonconformity can result in loss of certification.

Use the ISO 27001 ISMS Planning template in OneTrust to assist with ISMS decision-making according to Clauses 4-10 of the ISO/IEC 27001:2013 standard, including evaluating your organization and its context, understanding the needs and expectations of interested parties, determining the scope of the ISMS, identifying leadership roles and responsibilities, establishing and tracking objectives, defining risk criteria, and more.



Welcome

1 Context of the Organization

1.1 Understanding the organization and its context

1.2 Understanding the needs and expectations of interested parties

1.3 Determining the scope of the information security management system

1.4 Information security management system

Drag in a question tile from the left, or click to Create a Question

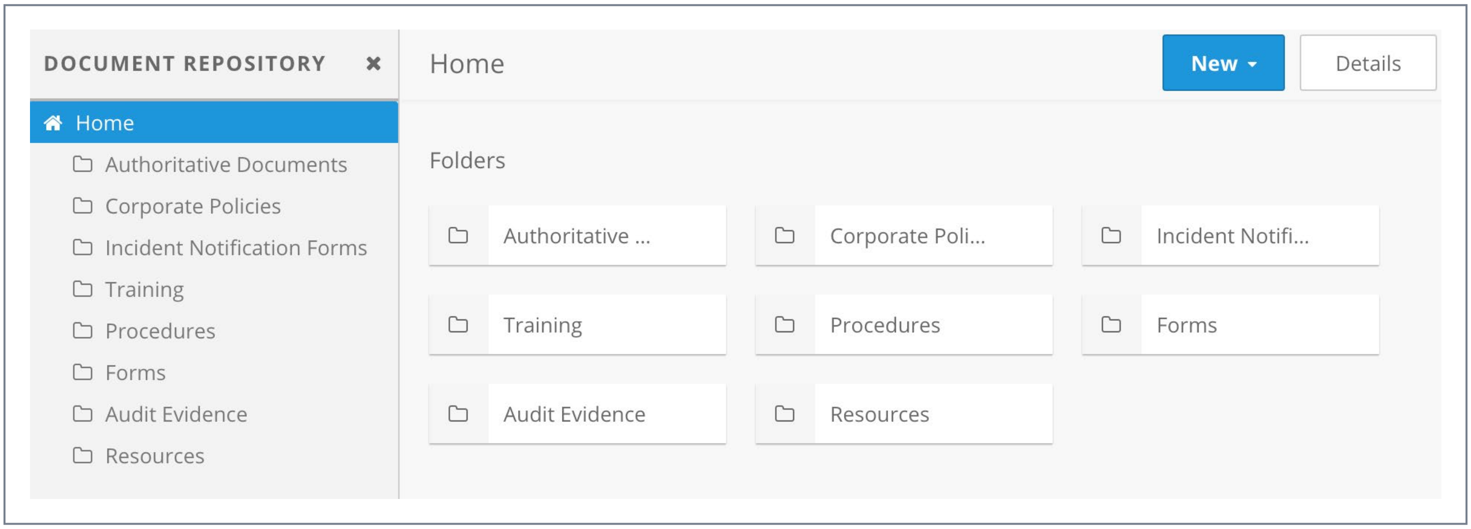
Customizable ISO 27001 ISMS Planning Template in OneTrust

Documentation

ISO 27001 requires a substantial amount of documentation to be created, reviewed, updated and properly controlled over the life of the ISMS. This documentation is vital to the effectiveness and continuous improvement of the ISMS, as well as to achieving and maintaining certification.

A common approach to storing documentation is to organize it according to the structure of the ISO/IEC 27001:2013 standard—e.g., folder containing core documents that address Clauses 4-10 of the standard, a folder containing policies and procedures specifically addressing applicable Annex A controls, a folder containing frequently used template documents (e.g., template agreements, incident reports, training slides, etc.), and a folder containing evidence of security operations and implementation.

Use the Document Repository in OneTrust to store and organize ISMS documentation in a central location for access by the ISMS team and other need-to-know personnel.

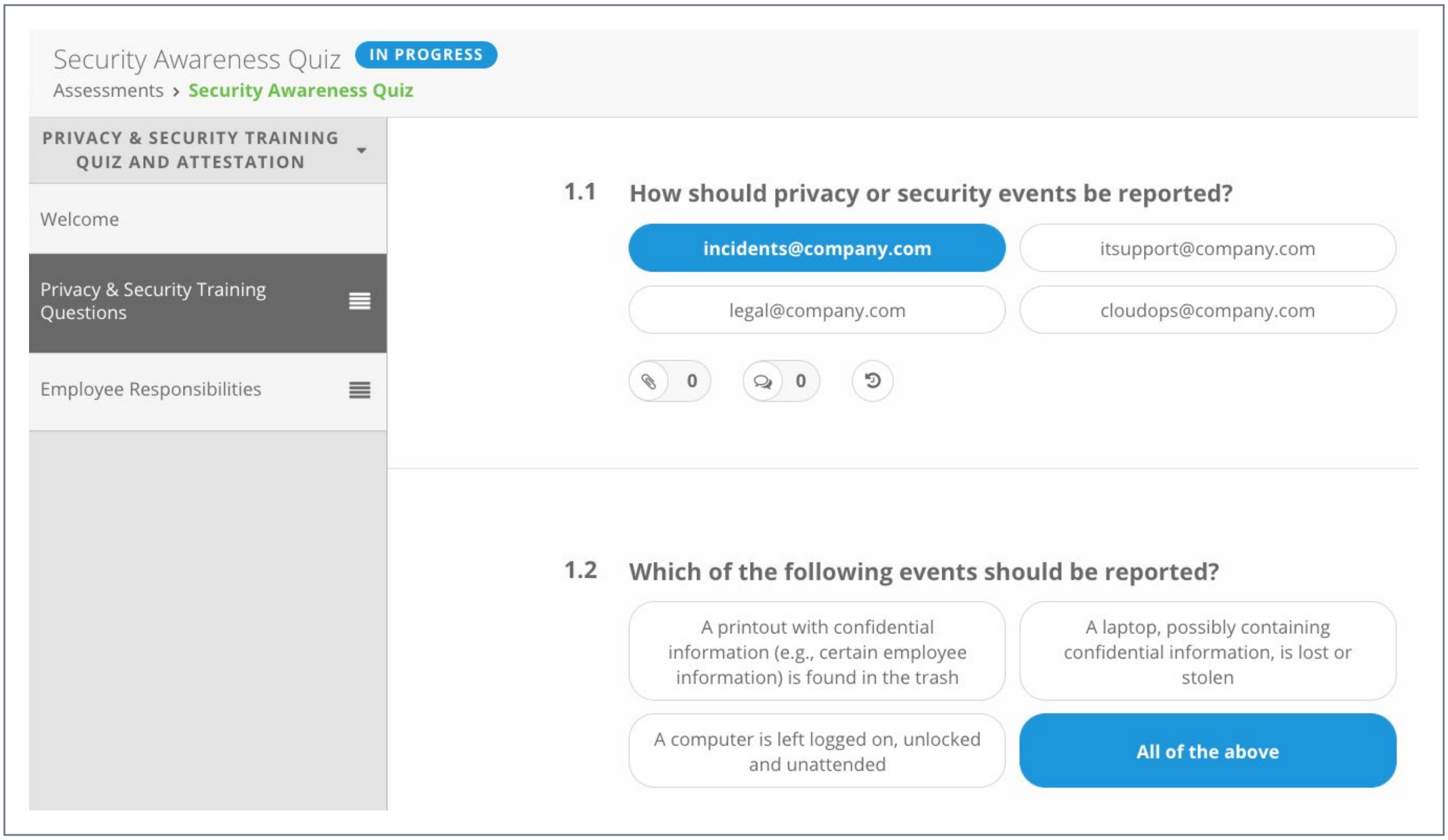


OneTrust Document Repository

Security Awareness Training, Testing and Attestation

Clause 7.3 requires that employees and contractors be made aware of the organization's information security policy, their individual contributions, roles and responsibilities in the ISMS, and the consequences of not conforming to requirements. Additionally, Annex A control A.7.2.2 requires that all employees and contractors receive information security awareness education and training, as well as regular updates on applicable policies and procedures.

OneTrust privacy and security training templates, such as the "Privacy and Security Training Quiz and Attestation" template, can be used to assist with testing the effectiveness of awareness training, as well as to record employee attestations to acceptable use policies or employee responsibility documents.


Security Awareness Quiz
IN PROGRESS
Assessments › Security Awareness Quiz
PRIVACY & SECURITY TRAINING QUIZ AND ATTESTATION
Welcome
Privacy & Security Training Questions
Employee Responsibilities
0
0

1.1 How should privacy or security events be reported?

[✓ incidents@company.com] itsupport@company.com legal@company.com cloudops@company.com

1.2 Which of the following events should be reported?

- A printout with confidential information (e.g., certain employee information) is found in the trash
- A laptop, possibly containing confidential information, is lost or stolen
- A computer is left logged on, unlocked and unattended
- [✓ All of the above]

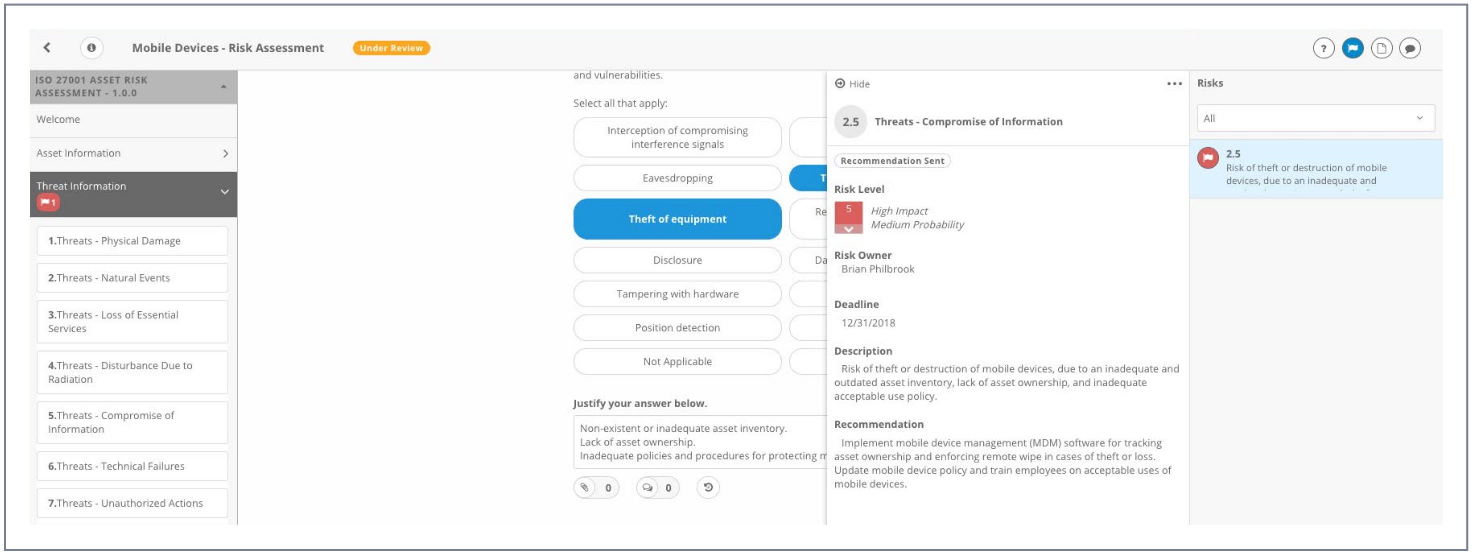
OneTrust Privacy and Security Training Templates

Risk Assessment and Treatment

Clause 6.1 requires the creation of a detailed risk assessment methodology that includes criteria for how to identify different levels of risk (i.e., what constitutes high versus low impact to the organization, and what types of risk is the organization comfortable with accepting), a procedure for creating and carrying out risk treatment plans, the frequency of risk assessments, and more.

Clause 8 then requires the implementation of these plans—i.e., following the risk methodology when conducting annual risk assessments, setting risk treatment plans and tracking them to completion, calculating residual risk, and ensuring that all of this is documented in a controlled manner.

OneTrust can be used to identify threats and vulnerabilities for information assets, or vendors, as well as to calculate risks, and to craft and track risk treatment plans. To get started, try the ISO 27001 Asset Risk Assessment template.


Mobile Devices - Risk Assessment
Under Review
ISO 27001 ASSET RISK ASSESSMENT - 1.0.0
Welcome
Asset Information
Threat Information
1
1.Threats - Physical Damage
2.Threats - Natural Events
3.Threats - Loss of Essential Services
4.Threats - Disturbance Due to Radiation
5.Threats - Compromise of Information
6.Threats - Technical Failures
7.Threats - Unauthorized Actions
Interception of compromising interference signals
Eavesdropping
T
Theft of equipment
Re
Disclosure
Da
Tampering with hardware
Position detection
Not Applicable
0
0
Hide
Risks
All

and vulnerabilities.

Select all that apply:

Justify your answer below.

Non-existent or inadequate asset inventory.
Lack of asset ownership.
Inadequate policies and procedures for protecting m

2.5 Threats - Compromise of Information

Recommendation Sent

Risk Level
5 *High Impact*
Medium Probability

Risk Owner
Brian Philbrook

Deadline
12/31/2018

Description
Risk of theft or destruction of mobile devices, due to an inadequate and outdated asset inventory, lack of asset ownership, and inadequate acceptable use policy.

Recommendation
Implement mobile device management (MDM) software for tracking asset ownership and enforcing remote wipe in cases of theft or loss. Update mobile device policy and train employees on acceptable uses of mobile devices.

2.5
Risk of theft or destruction of mobile devices, due to an inadequate and

Risk Review of Completed ISO 27001 Asset Risk Assessment Template

Statement of Applicability

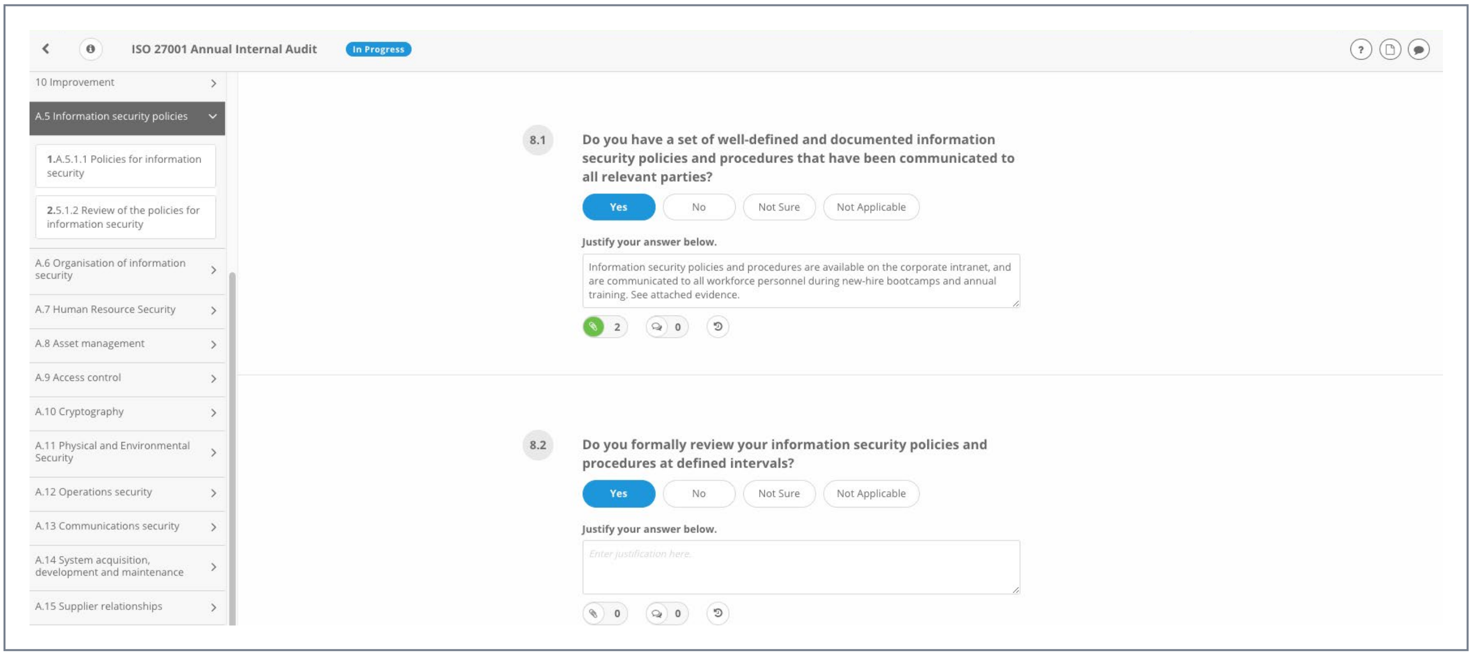
Clause 6.1.3 calls for the creation of a "statement of applicability" that documents the ISO 27001 Annex A controls that have been deemed applicable to the ISMS, based on a risk assessment, along with justifications for including and excluding certain controls.

When combined with risk assessment capabilities in OneTrust, the ISO 27001 Statement of Applicability template can be used to create this documentation with ease.

Internal Audits

Clause 9.2 requires that you conduct internal audits of the ISMS against the ISO/IEC 27001:2013 standard (including Clauses 4-10 and applicable Annex A controls). Moreover, Clause 9.3 calls for management reviews of the ISMS at planned intervals.

Use the ISO 27001 Audit Checklist template, a fully customizable questionnaire in OneTrust based on ISO 27001 to assist in conducting internal or external audits of the ISMS, to evaluate the maturity and overall effectiveness of the ISMS, and to track corrective action plans. After completing an audit, OneTrust allows you to easily generate an audit report showing an overview of your answers, comments and evidence attachments.



ISO 27001 Annual Internal Audit · In Progress

- 10 Improvement
- A.5 Information security policies
  - **1.**A.5.1.1 Policies for information security
  - **2.**5.1.2 Review of the policies for information security
- A.6 Organisation 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

8.1 Do you have a set of well-defined and documented information security policies and procedures that have been communicated to all relevant parties?

[✓ Yes] No Not Sure Not Applicable

Justify your answer below.

Information security policies and procedures are available on the corporate intranet, and are communicated to all workforce personnel during new-hire bootcamps and annual training. See attached evidence.

2 0

8.2 Do you formally review your information security policies and procedures at defined intervals?

[✓ Yes] No Not Sure Not Applicable

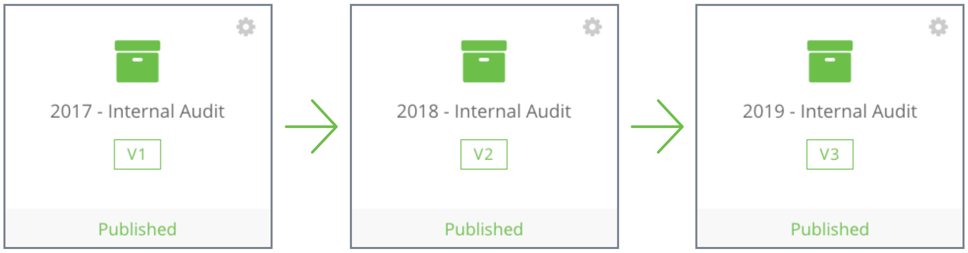
Justify your answer below.

Enter justification here.

0 0

ISO 27001 Audit Checklist Template

OneTrust is also great for documenting and demonstrating the continual improvement of an ISMS. With assessment versioning and reporting features, you can easily see how your program has grown year over year.

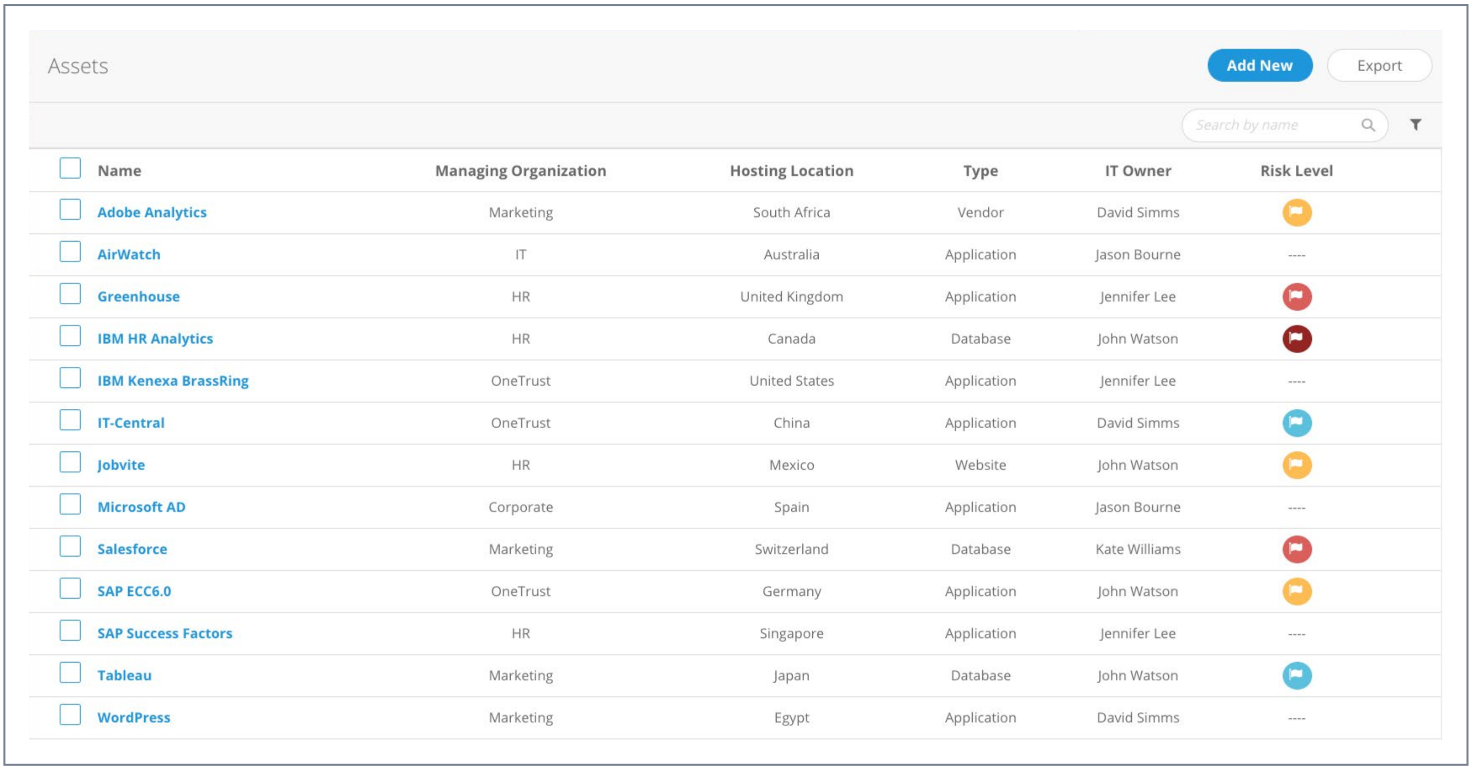


Assessment Versioning

Asset and Vendor Inventory

ISO 27001 Annex A controls A.8.1.1 and A.15.2 call for the development of asset and vendor/supplier inventories, respectively. Assets may include physical assets (e.g., hardware, mobile devices or facilities); process assets (e.g., human resource, recruiting or SDLC processes); technology assets (e.g., networks, databases or messaging tools); information assets (e.g., source code, intellectual property or customer data); or people assets (e.g., owners, employees and contractors).

With OneTrust, you can create and maintain inventories of your organization's assets and vendors, the risks associated with each, and their owners within the organization. Additionally, OneTrust automatically generates visualizations and data flow diagrams as tools for easier analysis and executive communication.



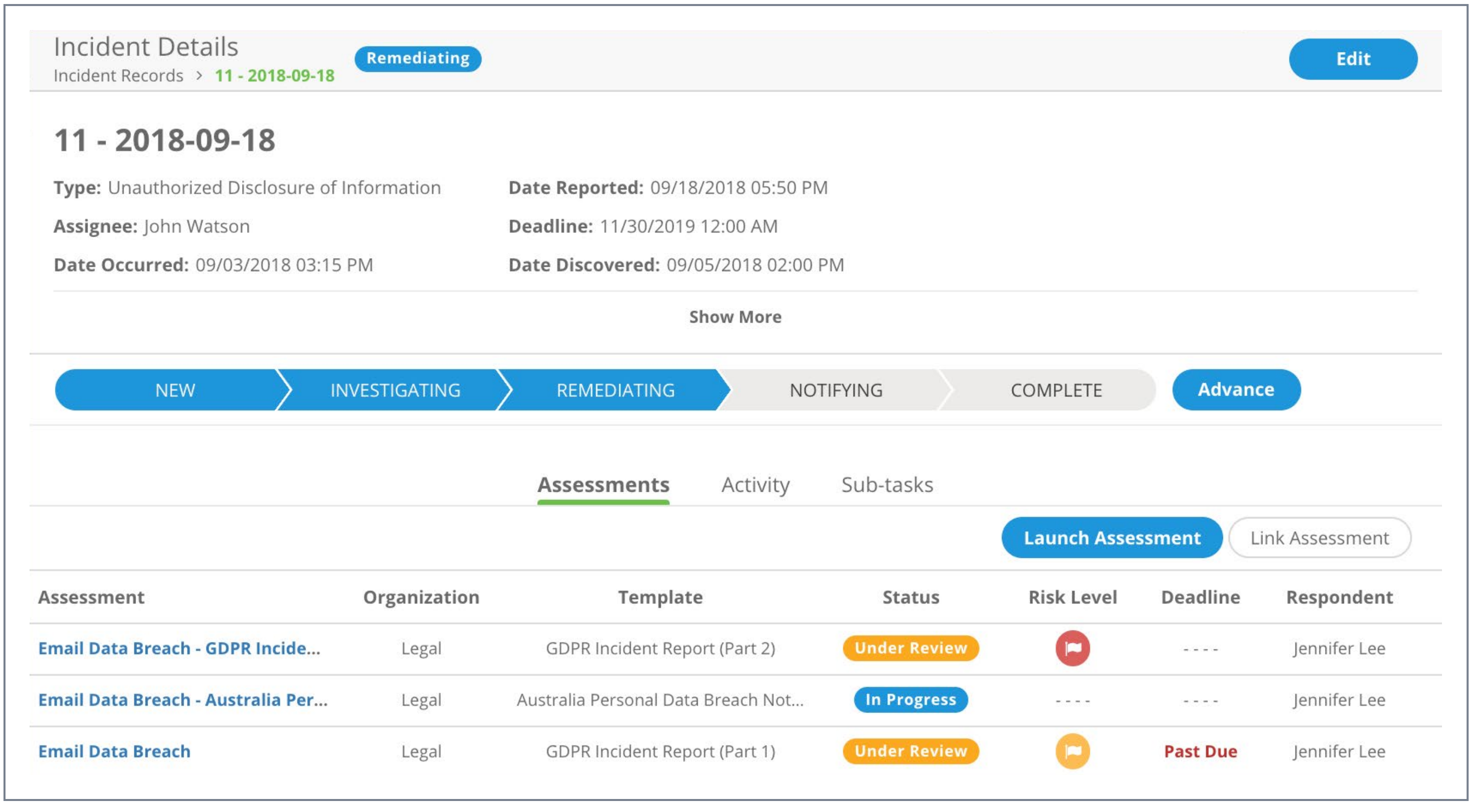
□	Name	Managing Organization	Hosting Location	Type	IT Owner	Risk Level
□	Adobe Analytics	Marketing	South Africa	Vendor	David Simms	🟠
□	AirWatch	IT	Australia	Application	Jason Bourne	----
□	Greenhouse	HR	United Kingdom	Application	Jennifer Lee	🔴
□	IBM HR Analytics	HR	Canada	Database	John Watson	🟤
□	IBM Kenexa BrassRing	OneTrust	United States	Application	Jennifer Lee	----
□	IT-Central	OneTrust	China	Application	David Simms	🔵
□	Jobvite	HR	Mexico	Website	John Watson	🟠
□	Microsoft AD	Corporate	Spain	Application	Jason Bourne	----
□	Salesforce	Marketing	Switzerland	Database	Kate Williams	🔴
□	SAP ECC6.0	OneTrust	Germany	Application	John Watson	🟠
□	SAP Success Factors	HR	Singapore	Application	Jennifer Lee	----
□	Tableau	Marketing	Japan	Database	John Watson	🔵
□	WordPress	Marketing	Egypt	Application	David Simms	----

OneTrust Asset Inventory

Incidents and Breaches

Annex A control 16 is all about information security incident management, including designating responsibilities and defining procedures for reporting, responding to, and learning from incidents. Additionally, A.16 requires organizations to maintain records of incidents and evidence demonstrating proper response in accordance with the organization's policies and procedures, as well as mitigation steps followed, and measures taken to prevent repeat incidents in the future.

With OneTrust, you can enable self-service reporting of security incidents and weaknesses, maintain incident and breach records, evaluate against breach notification obligations, and analyze overall risk with connections to your underlying inventories of data, processing activities, assets and vendors. OneTrust can be used to put incident management policies and procedures into action.



Incident Details

Incident Records > 11 - 2018-09-18

11 - 2018-09-18

Type: Unauthorized Disclosure of Information

Date Reported: 09/18/2018 05:50 PM

Assignee: John Watson

Deadline: 11/30/2019 12:00 AM

Date Occurred: 09/03/2018 03:15 PM

Date Discovered: 09/05/2018 02:00 PM

Assessment	Organization	Template	Status	Risk Level	Deadline	Respondent
Email Data Breach - GDPR Incide...	Legal	GDPR Incident Report (Part 2)	Under Review	⚑	- - - -	Jennifer Lee
Email Data Breach - Australia Per...	Legal	Australia Personal Data Breach Not...	In Progress	- - - -	- - - -	Jennifer Lee
Email Data Breach	Legal	GDPR Incident Report (Part 1)	Under Review	⚑	Past Due	Jennifer Lee

Customizable Incident & Breach Response Workflow

About OneTrust

OneTrust is the largest and most widely used dedicated privacy management technology platform for compliance with global privacy laws. More than 1,700 customers, including 200 of the Global 2,000, use OneTrust to comply with global data privacy regulations across sectors and jurisdictions, including the EU GDPR, ePrivacy (Cookie Law), the California Consumer Privacy Act and more. An additional 10,000 organizations use OneTrust's technology through a partnership with the International Association of Privacy Professionals (IAPP), the world's largest global information privacy community.

The comprehensive platform is based on a combination of intelligent scanning, regulator guidance-based questionnaires, automated workflows and developer plugins used together to automatically generate the record keeping required for an organization to demonstrate compliance to regulators and auditors. The platform is enriched with content from hundreds of templates based on the world-class privacy research conducted by our 300+ in-house certified privacy professionals.

The software, available in 50+ languages, is backed by 27 awarded patents and can be deployed in an EU cloud or on-premise.

OneTrust is co-headquartered in Atlanta, GA and in London, UK, with additional offices in Bangalore, Melbourne, Munich and Hong Kong. The fast-growing team of privacy and technology experts surpasses 500 employees worldwide. To learn more, visit OneTrust.com.

Privacy Program Management	Marketing Compliance Consent, Preferences, and Subject Rights	Vendor Risk Management	Incident and Breach Response
Assessment Automation PIA | DPIA | PbD | InfoSec	**Cookie Compliance** Web Scan & Consent Powered by Cookiepedia™	**Self-Service Assessments** CSA, SIG, VSA, Custom	**Incident Intake** Maintain Central Register
Data Mapping Automation Discovery, ROPA, Inventory	**Universal Consent** Central Records of Consent	**Vendorpedia™** Shared Intelligence and Scanning of Vendors	**Databreachpedia™** 300+ breach laws indexed
PbD Automation Automated PbD Checklists	**Universal Preference Center** End User Self-Service	**4th Party Management** Detect Sub-Processors	**Incident Risk Assessment** Analyse Risk and Harms
Global Regulatory Readiness Tracker Planning & Exec Dashboard	**Data Subject Rights Portal** End to End Automation	**Contract & DPA** Track Key Terms	**Notification & Reporting** Track Obligations

ONLINE DEMO AND FREE TRIAL **AT ONETRUST.COM**

OneTrust

Privacy Management Software

ONETRUST.COM

ATLANTA | LONDON | MELBOURNE | BANGALORE | MUNICH | HONG KONG

OneTrust is the global leader in privacy management and marketing compliance software. More than 1,700 customers, including 200 of the Global 2,000, use OneTrust to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR, ePrivacy (Cookie Law) and the California Consumer Privacy Act.