onetrust

OneTrust Tech Risk & Compliance Professional

Certification Program Handbook

The training environment assigned to you is only provided for training and certification purposes

You will have access to login for the duration of the training and approximatively 5 days after the training

URL: training.onetrust.com

Please refer to your instructor for the username/password to your assigned environment

Note: training.onetrust.com will redirect you to the most recent active version of the training environment, so the URL will change to either **training1.onetrust.com** or **training2.onetrust.com**

Contents

OneTrust Tech Risk & Compliance Professional Certification Program Reference Guide

Prepared for:

OneTrust Tech Risk & Compliance Professional Certification Attendees

Version 202405.2.4

Introduction

Welcome to the OneTrust Tech Risk & Compliance Certification Program Reference Guide, your comprehensive guide to becoming a certified OneTrust GRC professional.

While OneTrust is the leading global software to operationalize data privacy compliance and Privacy by Design, OneTrust also offers a Governance, Risk, and Compliance solution (GRC). OneTrust GRC Integrated Risk Management is a suite of integrated risk management products to identify, measure, mitigate, monitor, and report on risk across operations.

Legal Disclaimers

The contents of this document may be revised by OneTrust in its sole discretion, without notice, due to continued progress in the methodology of the Certification, any changes in applicable laws, regulations or related guidance, or for any other reason. OneTrust shall have no liability for any error or damage of any kind resulting from the use of this document, its contents or the information provided therewith.

The contents of this document, any materials and other information conveyed during this Tech Risk & Compliance Professional Certification are for informational purposes only and do not constitute legal advice (and should not be relied upon as such).

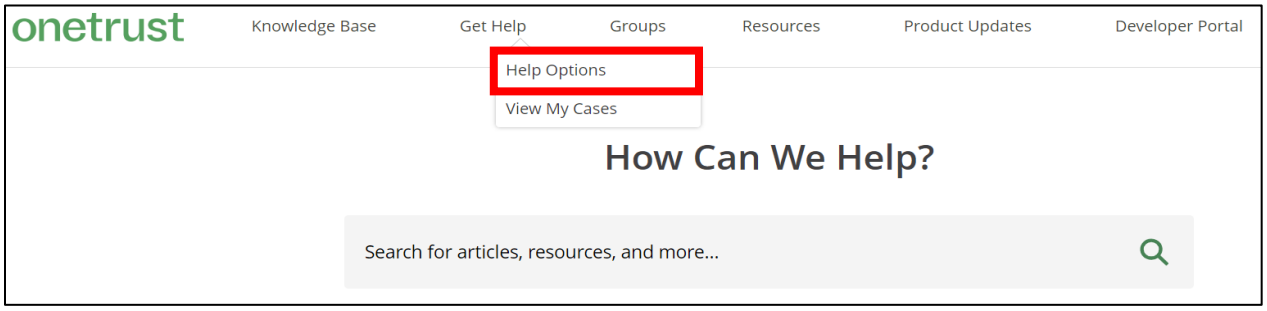
Resources & Support

Sales

- Email: Sales@onetrust.com
- Phone Numbers:
  - *London:* +44 (800) 011-9778
  - *Atlanta:* +1 (844) 228-4440
  - *Munich:* +49 (175) 371-2983

Technical & Partner Support

- For Partners, your first point of contact should be your Partner Representative
- Technical and other support cases can be made directly in My.OneTrust.com by selecting the option below:



MyOneTrust

- Website: my.OneTrust.com

My OneTrust is a platform that can be accessed by all OneTrust customers for additional resources which include, but it not limited to:

1. OneTrust Knowledge
2. Release Notes
3. Schedule Maintenance
4. Live System Status
5. Submit a Ticket
6. Developer Portal
7. Get OneTrust Certified

Training & Certifications

- For general inquires and questions about instructor-led courses, email Training@OneTrust.com
- For inquiries regarding our eLearning courses, contact eLearning@OneTrust.com

Terminology & Frameworks Overview

What is Governance?

Governance is defined as the way rules, norms, and actions are **structured**, **sustained**, **regulated**, and **held accountable**.

Governance Initiatives

What is Risk?

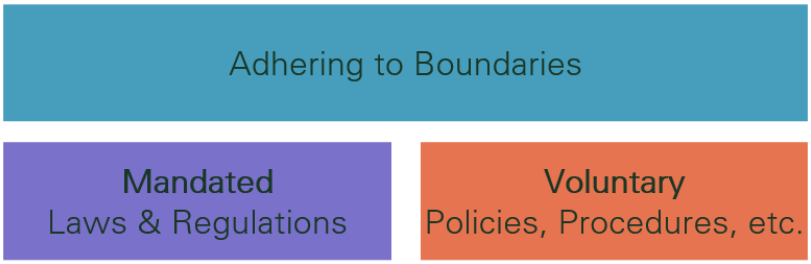
Risk is defined as the possibility or chance of **loss**, **adverse effect(s)**, **danger**, or **injury**.

Risk Initiatives

What is Compliance?

Compliance is the act of ensuring your company and employees **follow the laws**, **regulations**, **standards**, and **ethical practices** that apply to your organization.

Compliance Initiatives



Common Terminology

- Security Standards/Framework - A series of documented **processes** that are used to define **policies and procedures** around the implementation and ongoing **management of information security controls** in an enterprise environment
- Controls Library - Includes controls from **recognized frameworks** and **custom controls** which your organization can use to **evaluate** and **describe** the security and privacy requirements you have for vendors within the OneTrust application
- Control Implementations - **Safeguards** or **countermeasure** to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. An organization can use controls to **evaluate** and **describe** the security and privacy requirements necessary for vendors.

Commonly Used Frameworks

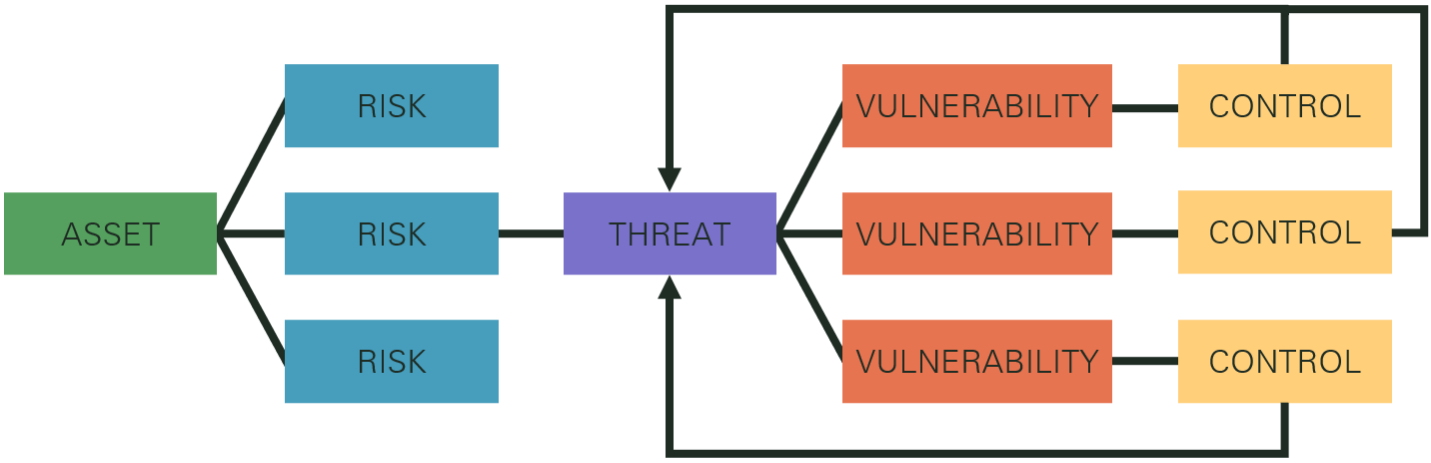
Name	Abbreviation	Industry
Cloud Security Alliance / Cloud Controls Matrix	CSA CCM	Cloud Computing Environments
Federal Risk & Authorization Management Program	FedRAMP	Government-wide approach to security assessment, authorization, & monitoring for cloud products & services
International Organization for Standardization	ISO27001	Information Security Management Systems (ISMS) Issued & maintained by the International Organization for Standardization
National Institute of Standards & Technology Publication 800-53	NIST 800-53	United States federal information systems (excluding those related to national security)
Center for Internet Security	CIS Controls	Computer & Cyber Security
American Institute of Certified Public Accountants' Trust Services Criteria Service Organization Control 2	AICPA TSC SOC2	Audit procedure to ensure protection of sensitive data

IT Risk Management: Elements & Inventories

IT Risk Management is defined as the set of **Policies**, **Procedures**, as well as the **technology** that an organization puts into place to **reduce threats**, **vulnerabilities**, and **other results** caused by having **unprotected data**. OneTrust can assist our customers' IT Risk Management efforts by **supplying efficient tools** to define and track risks to apply mitigating measures towards those risks. This chapter focuses on anticipating common risks that your organization may face and preparing the tool to be ready to manage these risks by thoroughly configuring your Controls Library, Elements, and Inventories.

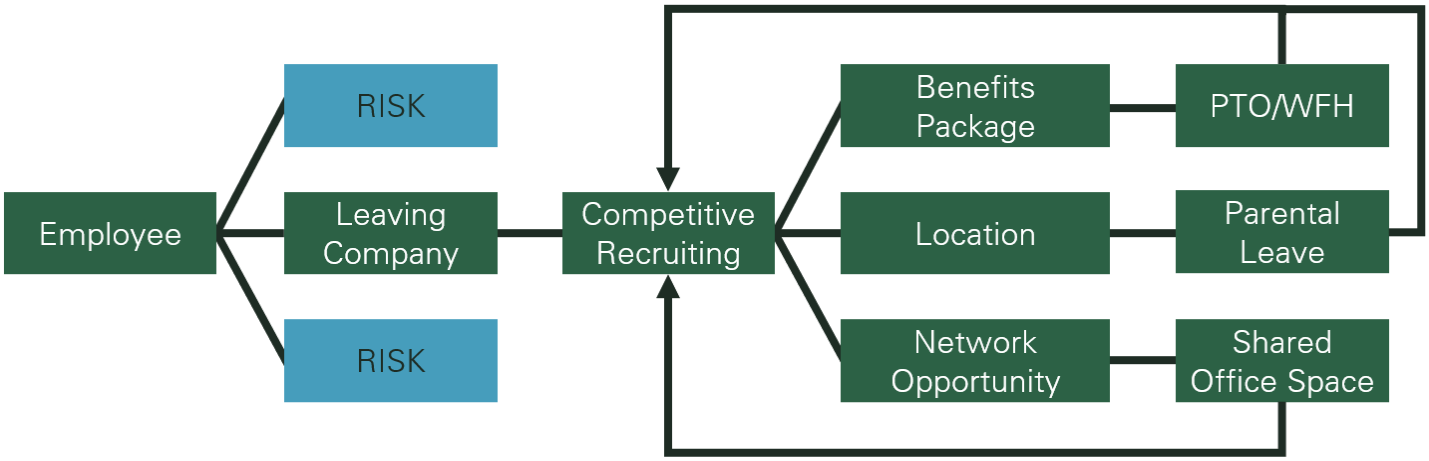
Tool Overview

Elements



- **Asset** – any item of value to your business
- **Risk** – potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability
- **Threat** – anything that can exploit a vulnerability, either intentionally or accidentally, and obtain damage or destroy an asset
- **Vulnerability** – a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset
- **Control** – an attribute or element (either real or conceptual) that acts as a mitigating factor to reduce risk

Elements Example



Inventories

Inventory	Definition	Risk Example	Control Example
Assets	Any item of value to a business, whether physical or abstract.	Asset creates tickets that contain sensitive information.	Encrypt ticket information with key stored in a separate database.
Processing Activities	Any activity where data is touched, stored, or moved.	Mobile devices used don't have multi-factor authentication enabled.	Update mobile device policy to include MFA requirements.
Entities	A registered business involved in and responsible for data processing.	Not trained on internal controls framework.	Implement mandatory training policy.
Vendors	A third-party service provider.	Current policy for data breaches is outdated.	Set up quarterly reminders for business to follow up with vendor for updated policy.

Considerations

Execution

Risk Scoring Methodology

OneTrust includes a couple risk scoring methodologies. The selected method would need to be decided and understood across several teams. When using the Risk Scoring Matrix, several items of that matrix can be configured to meet your organization's needs.

Detailed Exercise Steps

Step 1: Click the **gear icon** in the top right and scroll down the all the way to the bottom of the left menu

Step 2: Select the **Risk Scoring** tab in the **Risk & Controls** section

Step 3: Click the **Scoring Methodology dropdown** and select either **Matrix** or **Standard**

Note: If you choose Standard, the next steps are not necessary

Step 4: If you chose **Matrix**, click the **plus buttons** to add a new column and row – label them both **Urgent**

Step 5: Make the furthest **top right square** "9" instead of "8"

Step 6: Scroll down to the **Risk Level Ranges** bar and drag the **yellow** marker to 4, the **pink** marker to 6, and the **red** marker to 8.

Step 7: Click the **Save** button at the bottom right and again on the pop-up window

Adding Controls

The OneTrust Tool provides users with a Controls Library with the ability to add controls from multiple standards/frameworks or from scratch to be associated with inventory items such as Assets, Processing Activities, Vendors, Entities, and Risks, themselves. The controls in this library also extend into other GRC modules, such as Audit Management.

Detailed Exercise Steps

Part 1

Step 1: Click the **Launch Pad** at the top left of the screen

Step 2: Click on the **IT & Security Risk Management** module

Step 3: Select the **Controls Library** tab in the **Libraries** section on the left menu

Step 4: Click the **Add New** button at the top right of the screen

Step 5: For **Control ID**, type **A.9 4.3 (2)**

Step 6: For **Name**, type **Password Management System**

Step 7: For **Status**, select **Active**

Step 8: For **Standard/Framework**, select **ISO/IEC 27001:2013 (27002)** from the list

Step 9: Click the **Save** button at the bottom right of the menu

Part 2

Step 1: Click the **Add Standard/Framework** button at the top right of the screen

Step 2: Type **NIST** into the search bar at the top right of the screen and click enter

Step 3: Click on **NIST CSF (Cybersecurity Framework) v1.1**

Step 4: Click the **Add** button at the bottom right of the menu

Create an Asset & Processing Activity

While there are multiple ways to add inventory items, this exercise will use the manual interface. The OneTrust tool gives our customers the ability not only to add and track inventory items, but to relate them together to create a web of information. Risks are then able to be applied to all of these individual inventory items, no matter the type.

Detailed Exercise Steps

Part 1

Step 1: Click the **Assets** tab on the left menu under the **Inventory** section

Step 2: Click the **Add New** button at the top right of the screen

Step 3: For **Name**, type **Payroll Database**

Step 4: For **Managing Organization**, select **OneTrust**

Step 5: For **Hosting Location**, select a **country of your choice**

Step 6: For **Type**, select **Database** from the list

Step 7: Click the **Save** button at the bottom right of the menu

Part 2

Step 1: Click the **Processing Activities** tab on the left menu under the **Inventory** section

Step 2: Click the **Add New** button at the top right of the screen

Step 3: For **Name**, type in **Monthly Compensation Calculation**

Step 4: For **Managing Organization**, select **OneTrust**

Step 5: Click the **Save** button at the bottom right of the menu

Part 3

NOTE: The related tab may look different if you are already working with the OneTrust tool.

Step 1: Click the **Related** tab across the top within the **Processing Activity** from **Part 2**

Step 2: Scroll down to the **Related Assets** section and click **Add Related Asset**

Step 3: Click the **Choose an asset** box and select the **asset you created** in Part 1

Step 4: Check the **Related** box under the **How is asset related?** section

Step 5: Click the **Add Related** button

Prepare for Common Risks

Once inventory items are configured and business processes determined, Assessment Templates should be reviewed and/or created. Within these templates, identifications of question responses that could mean risk should be made. For these answers, rules can be put in place to auto-create risks in the system with pre-assigned controls for swift management.

Detailed Exercise Steps

Part 1

Step 1: Find the **Setup** section on the left menu

Step 2: Click the **Templates** tab within

Step 3: Click the **View** button in the **ITRM Templates** box

Step 4: Click the **Choose from Gallery** button in the top right

Step 5: Type **Asset Discovery** in the search bar at the top

Step 6: Hover over **Asset Discovery Questionnaire – 2.4** and click the **Preview** button

Step 7: Click **Choose This Template** in the bottom right

Step 8: **Add your initials** to the front of the name (XXX – Asset Discovery Questionnaire – 2.4)

Step 9: Click **Create Template** in the bottom right

Part 2

Step 1: Click the **arrow** to the far right of the first section (**Asset Information**) to view all the questions within.

Step 2: Drag the **Yes/No Question Type** box from the left and drop it in between questions 1.1 and 1.2 (make sure to drop it in the blue box that appears that reads **Drop Question Here**)

Step 3: In the **Question** field, type **Is access to this asset restricted to only individuals that require access?**

Step 4: Click the **Save** button in the bottom right

Part 3

Step 1: Click the **Rules** tab near the top of the screen & click the **Add Rule** button

Step 2: **Name** the rule **No Access Control**

Step 3: Populate the **Trigger** box with **Question**

Step 4: Populate the newly clickable **Question** box with the **Yes/No question you just created**

Step 5: Populate the **Operator** box with **Equal To**

Step 6: Populate the **Response** box with **No**

Step 7: In the **Select an Action** box, choose **Create Risk**

Step 8: Click the circle for **Create New Risk**

Step 9: Give the risk an **Inherent Risk Level** & **Description** (Access to asset is not limited to only those that require access.)

Step 10: Click the **Add Risk Control** button near the bottom & select **ISO/IEC 27001:2013 (27002)** on the left

Step 11: Check the boxes for **A.9: Access Control** and **A9.1.1: Access Control Policy** then click **Add**

Step 12: Click **Save** in the bottom right

Step 13: Click **Publish** in the top right

Step 14: Click **Confirm** near the middle

IT Risk Management: Assessment & Risk Management

In this module, we focus on using GRC Assessments to obtain information about our inventory items and identify risks as well as mitigating these risks by use of the Risk Lifecycle.

Overview

A **GRC Assessment** can be defined as a survey that gathers evidence to determine risk. In simple form, GRC assessments verify answers and provide access to key data:

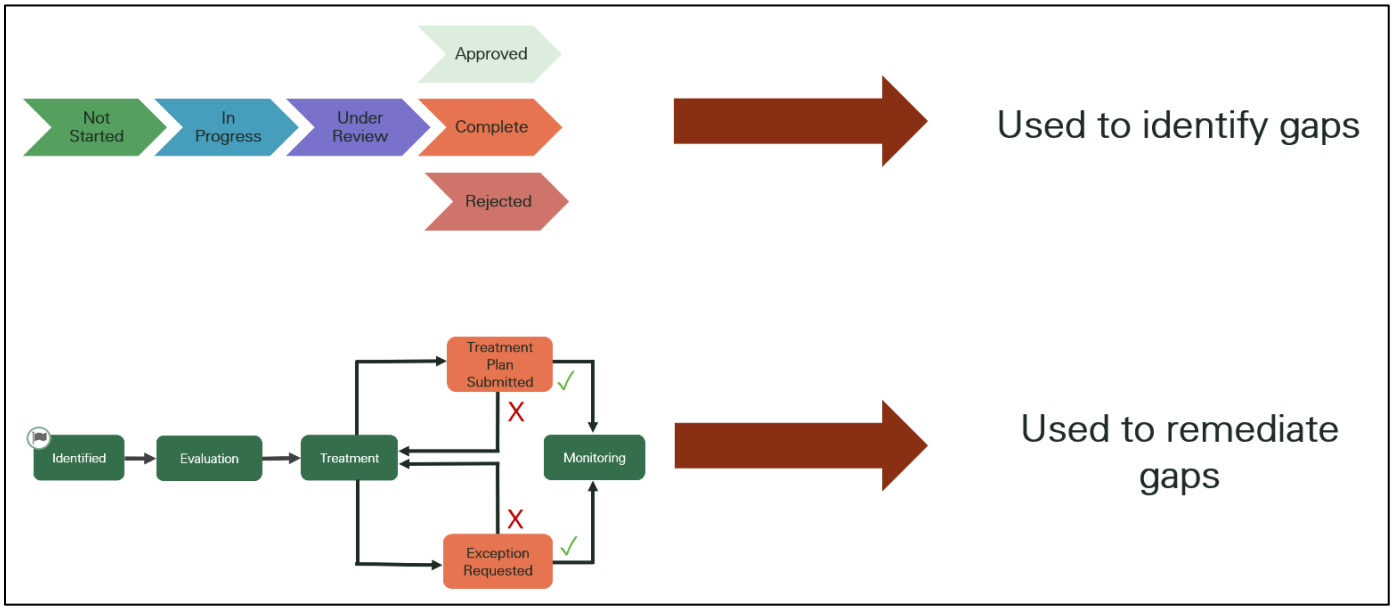
- Is this control implemented?
- Attach piece of evidence
- Explain

Example

ISO 27001: the international standard that describes **best practices** for **implementing** and **maintaining** an ISMS (**information security management system**). An ISO27001 Risk Assessment is essential to that process and is a core component of this standard. This type of risk assessment helps organizations:

- **Understand** specific scenarios that would result in their data being compromised
- **Assess** the damages these scenarios could cause
- **Determine** how the likelihood of these scenarios happening

Assessment & Risk Lifecycles



Considerations

Execution

Delivering Assessments

Once the best respondents have been determined, we need to send them the questionnaire template we created previously. Once a template is sent to a respondent, it's called an Assessment. In this exercise, we will launch an assessment to ourselves so that we can then see the Respondent's side of how to complete and submit the answers to an approver.

Detailed Exercise Steps

Part 1

Step 1: Click on the **Active** tab under the **Assessments** section on the left menu

Step 2: Click the **Launch Assessment** button at the top right of the screen

Step 3: Select the **Template** you previously published

Step 4: For **Name**, enter **Payroll Database Required Review**

Step 5: For **Organization**, select **OneTrust**

Step 6: For **Primary Record Type**, select **Assets**

Step 7: For **Primary Record**, select the asset you created (Payroll Database) from the list

Step 8: Select **yourself** (Admin###) for both **Respondent** and **Approver**

Step 9: Click the **Launch** button at the bottom right of the screen

Part 2

Step 1: Click the **Asset Information** section on the left

Step 2: Answer the **question you created** with **No**

Step 3: Answer a few more questions (main question requiring an answer is the one you created)

Step 4: Click the **Submit** button in the bottom right

Step 5: Click the **Confirm** button

Managing Risks

Assessment responses can trigger the system to auto-create risks because of built in rule logic which means the next step is to remediate the risk.

Detailed Exercise Steps

Step 1: Click the **Risk Register** tab on the left menu

Step 2: Click the **ID** of the risk that got created by submitting the assessment **(#189)**

Step 3: Advance your risk to the **Treatment** phase by clicking **Advance**

Step 4: Enter a **Risk Owner (Assign to Me)** and a **Treatment Plan** of your choice (Ex: Create and assign an access control policy to this asset)

Step 5: Click the **Save & Advance** button

Step 6: At the top right of the screen, click the **Request Exception** button.

Step 7: For comments, enter **Access to this database is open for all, but within the asset there are restricted areas to select employees.**

Step 8: Click the **Submit** button

Step 9: Click the **Grant Exception** button at the top right of the screen menu.

Step 10: For **Result**, select **Reduced**, or a result of your choice

Step 11: Change the **Residual Risk Level** to a lower score

Step 12: Click the **Confirm** button

Configure Automation Rule

Now that we've sent an assessment, have gotten it answered, then identified and managed a risk, we want to make sure we continue to monitor both the risk and inventory items in the future. To do this, we can automate the sending of assessments by use of various triggers. When that trigger (called a Condition) is met, the system will send another assessment to the specified respondent and the processes we've practiced in this lesson will continue.

Detailed Exercise Steps

Part 1

Step 1: Click the **Automation Rules** tab under the **Setup** section on the left menu

Step 2: Click the **Add Rule Group** button at the top right of the screen

Step 3: For **Rule Group Name**, enter **Asset Rule Group**

Step 4: For **Organization**, select **OneTrust**

Step 5: Click the **Add** button at the bottom right of the menu

Part 2

Step 1: Click the **Add Rule** button at the center of the screen

Step 2: For the **Select a Rule Type** dropdown, select **Asset**

Step 3: Click the **Continue** button

Step 4: For **Rule Name**, type in **Asset Review Rule**

Step 5: For **Frequency Run** on the drop-down menu select **Daily**

Step 6: For the **Trigger** dropdown, select **Last Assessment Completion Date – By Template**.

Step 7: For **Operator** dropdown, select **Equal To**.

Step 8: For **Number**, enter **180** (180 days are approximately 6 months)

Step 9: Click the **Select a Template** field and click the template name that you chose earlier

Step 10: For the **Actions** dropdown, select **Send Asset Assessment**

Step 11: Click into the **Template Name** field & select the **template you created earlier**

Step 12: Click the **Save** button at the bottom right of the screen.

Enterprise Policy Management

The Enterprise Policy Management module provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and best practices. The policy inventory is used to capture internal policies for an organization.

Policies can also be linked to controls, related to an inventory, and you can manage all policies centrally in one location. Policies help with managing the end-to-end policy workflow, from the creation of new policies to retiring policies that are no longer needed.

Overview

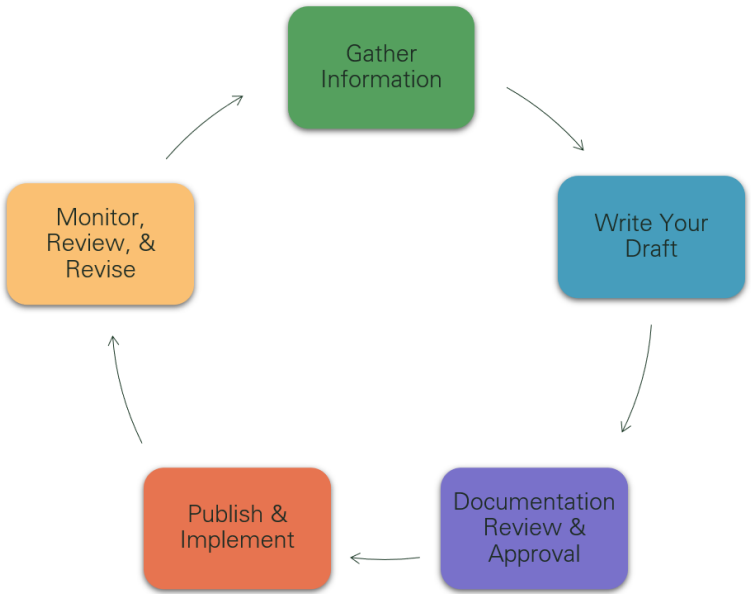
What do policies do?

Clarify expected output & behavior of an organization's members in the context specific to that organization (groups can include employees, volunteers, and other members (board members, etc.)

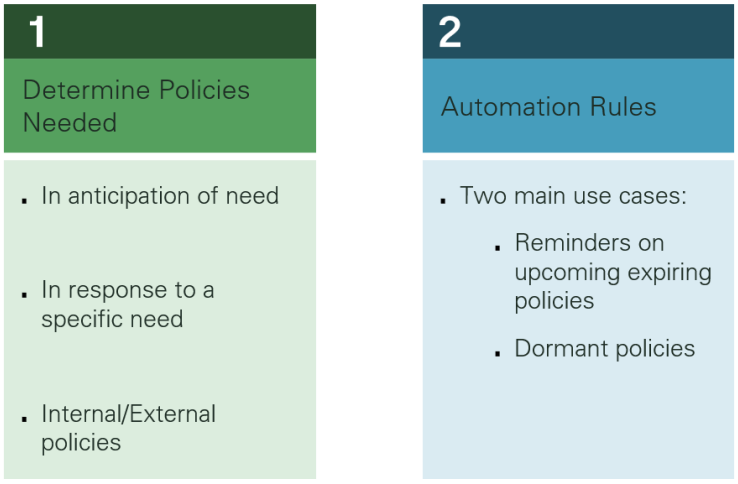
Why do we need them?

- Guide daily workplace activities
- Promote Compliance with laws & regulations
- Provide Strategic viewpoint of decision making
- Aid in simplification of processes

Policy Workflow



Considerations



Execution

Add a New Policy

Policies can be created in OneTrust through various methods, including loaded in via template, built from scratch, or by editing a pre-built template within the tool. These policies can then be edited, revised, reported on, and linked with controls to define processes of different types that your organization practices to keep GRC protocols top of mind.

Detailed Exercise Steps

Step 1: Click on the **Launch Pad** at the top left of the screen
Step 2: Click on the **Enterprise Policy Management** module
Step 3: Click the **Policies** tab on the left side of the screen
Step 4: Click the **Create Policy** button at the top right of the screen
Step 5: Select the **Choose from Templates** option then click **Next**
Step 6: Click the **Choose From Gallery** button in the top right corner
Step 7: In the **Search Bar**, type **Database**
Step 8: Hover over the **SANS Database Credentials Coding Policy** tile and click the **Preview** button
Step 9: Scroll through the contents then click the **Choose Policy** button at the bottom right
Step 10: For **Policy Name**, type **Database Credentials Policy**
Step 11: For **Managing Organization**, select **OneTrust**
Step 12: Select yourself as **Policy Owner** and **Policy Approver**
Step 13: Click the **Create** button at the bottom right of the menu

Add Controls to a Policy

Once policies are created, they can be linked with controls to ensure proper implementation and continued efficacy. Those controls can be from a Standard/Framework or ones that were manually configured in the Controls Library (as was demonstrated the IT Risk Management module).

Detailed Exercise Steps

Step 1: Click on the **Policies** tab on the left menu

Step 2: Click on the **Policy** you created

Step 3: Click on the **Controls** tab at the top middle of the screen

Step 4: Click the **Add Control** button in the center of the screen

Step 5: For **Standard/Framework**, select **ISO/IEC 27001:2013 (27002)** on the left side of the menu

Step 6: In the **Search Bar** at the top right, type **A9**

Step 7: Check the box for **A9.1.1 Access Control Policy**

Step 8: Scroll down to and check the box for **A9.2 User Access Management**

Step 9: In the **Search Bar** at the top right, type in **A.9**

Step 10: Check the box for **A.9 Access Control**

Step 11: Click the **Add** button at the bottom right of the menu

Relate Policy to a Vendor

Policies can extend beyond the bounds of the organization and look outward towards relationships with vendors. Similar to how risks can be linked to inventory items, or even how controls can be linked to Policies, Policies can be linked to Vendors that have been added to the Vendor Inventory.

Detailed Exercise Steps

Step 1: Click on the **Related** tab for your policy

Step 2: Scroll down and click the **Add Related Vendor** button

Step 3: Click on **Choose Vendor** and select a **Vendor of your choice**

Step 4: Click the **Add Related** button

Create an Automation Rule

As the workflow in the overview shows, Policies eventually come to an end. This could be due to the end of a process or because it's time to review and update the details. No matter the reason, a rule can be created in the system that will automatically remind specified users when a policy is coming up on its expiration date and is configured similarly to how we created risks to be auto-created through assessments.

Detailed Exercise Steps

Step 1: On the left menu, select **Automation Rules** under the **Setup** section

Step 2: Click the **Add Rule Group** button in the top right

Step 3: For **Rule Group Name**, type **Policy Rules**

Step 4: Select **OneTrust** as the **Organization**

Step 5: Click the **Add** button

Step 6: Click the **Add Rule** button

Step 7: Select **Policy** on the rule type drop down

Step 8: Click the **Continue** button

Step 9: For **Rule** name, type **Policy Reminder**

Step 10: Select **Daily** as the **Frequency**, click the black arrow to the right, then select a time of day of your choice

Step 11: Under **Conditions**, set the **Trigger** as **Attribute**

Step 12: Select **Effective Date** for the **Select Attribute** box

Step 13: Select **Equal To** for the **Operator**

Step 14: Add **7** for the **Number** box

Step 15: Keep the **Days Before** option

Step 16: Under **Actions**, select **Send Approval Reminder Email** from the drop down

Step 17: Click the **Save** button in the bottom right

Incidents Management

When incidents occur, it's best to have the means to respond to and mitigate them. This module includes a module overview, best practices, and practical steps within the tool to help organizations manage incident recording, notification, processing, as well as useful associations for mitigation.

Overview

Networks and Information System Directive → Information Commissioner's Office

General Data Protection Regulation → Supervisory Authority

Organizations must display **responsibility for ensuring implementation** of adequate security measures per certain regulations/initiatives	**Authorities must be contacted in no later than 72 hours** after organization becomes aware of breach	Consequences for contractual failure or missed deadlines can include **regulatory investigation and significant financial penalties**

A Breach Response Plan is a continually tested guideline for organizations to follow each time a breach is discovered. It should determine:

- Specific recording methods
- Directly Responsible Individuals (DRIs)
- Designated workflows

Considerations

1 Streamline Incident Reporting

- Web Forms to report Incidents
- Assessments to gather additional information & detailed descriptions of events

2 Assign Risks to Specific Owners

- Centralize communication
- Track accountability
- Improve response times

Execution

Create a Custom Incident Type

Incident Types not only provide details about the incident that occurred, but can also be used to drive automation within an incident workflow, as we'll see in the next exercise. If there's an incident type that you expect to encounter that not an out-of-box option in OneTrust, you can create this type in the platform. Creating a new type will automatically update the attribute, thus updating any attribute question type used for this purpose.

Detailed Exercise Steps

Step 1: Click the **Launch Pad** in the top left and select the **Incident Management** module

Step 2: Under **Setup** on the left menu, click on **Incident Types** tab

Step 3: Click the **Add New** button

Step 4: Add a new **Incident Type** option, for example: **Natural Disaster**

Step 5: Click the white **Add** button and then the **Save Attribute** button

Create an Incident Workflow

Incident Workflows are a series of configurable steps that help organizations manage incidents with rule-based notifications, tasks, attachments, a centralized communication portal, and more with the ability to assign specific owners to key items. All these tools allow for teams to properly mitigate incidents, and their associate risks, in a timely fashion. Organizations can create multiple workflows to meet the variety of incidents that can occur.

Detailed Exercise Steps

Part 1

Step 1: Click the **Workflows & Rules** tab in the **Setup** section on the left menu

Step 2: Click **Default Workflow**

Step 3: Click the **Clone** button at the top right

Step 4: For workflow name, type in **Data Incident Workflow**

Step 5: Click the **Clone** button

Part 2

Step 1: Click into **your new workflow**

Step 2: At the top middle of the screen, click the **+ button** in between **Investigating** and **Remediating**

Step 3: For stage name, type **Risk Analysis**

Step 4: Click the **Add** button at the bottom right of the menu

Step 5: Click on the **Rules** tab

Step 6: Click the **Add Rule** button in the center of the screen

Step 7: For **Rule Name**, type in **Notification Rule**

Step 8: For the **Actions** dropdown, select **Send Notification**

Step 9: For recipients, set the dropdown to **System User** then type in your email and click **Assign to: <your email>** option in the dropdown list

Step 10: For **Subject**, type **Data Incident Occurrence – Notify CIO**

Step 11: For **Body**, type **There has been a data incident, please visit the incident register for more details**

Step 12: Click the **Save** button at the bottom right of the screen

Step 13: Click the **Publish** button at the top right of the screen

Step 14: Click the **Publish** button in the center of the screen

Part 3

Step 1: Click the **Workflows & Rules** tab on the left side of the screen

Step 2: Click the **… button** to the far right of your new workflow

Step 3: Select **Set as default**

Step 4: Click the **Confirm** button

Create a New Attribute & Web Form

The Attribute Manager allows users to create and view attributes (both active and inactive) and create new custom attributes. Active attributes can be added to assessments to gather more information about the incidents. Users can also group like attributes to appear during the incident creation on the details screen.

Web Forms can be built within OneTrust and used by external users via a link or a website, if it has been embedded, to submit incidents directly to the Incident Register.

Detailed Exercise Steps

Part 1

Step 1: Click the **Attribute Manager** tab in the **Setup** section on the left menu

Step 2: Click the **Add Attribute** button

Step 3: Add a **Name** for the new attribute (**Incident Location**)

Step 4: Add a **Description** as a question (**Where did the incident happen?**)

Step 5: For **Response Type**, choose **Single Select** and add **3 cities** on the right for options

Step 6: Click on the **Save** button

Part 2

Step 1: Click the **Web Forms** tab under the **Setup** section on the left menu

Step 2: Click the **Add New** button in the top right

Step 3: Add a **name** (OneTrust Web Form) and click the **Create** button

Step 4: For **Form Fields** section, add the following: **Date Discovered**, **Data Occurred**, **Description**, **Incident Type**, and the **new attribute you created**

Step 5: In the **Form Styling** section, personalize your new **Web Form header** by adding a **logo** and **changing the color**

Step 6: OPTIONAL – Edit the text in the **Form Text** section

Step 7: Click on the **Save Template** button in the top right

Step 8: Click on the **Publish** button in the top right and then the center of the screen

Step 9: Click on the **Test** button on the window that appears

Step 10: Fill in the fields and click **Submit**

Step 11: **Exit the tab** to return back to the original screen

Link an Incident to a Risk

Users can easily view and manage all associated risks to an incident by linking the two together in the Risk Register.

Detailed Exercise Steps

Step 1: Click the **Incident Register** tab on the left menu

Step 2: Click into the **incident that was created in the previous exercise**

Step 3: Click on the **Risk Analysis** stage across the top and click **Continue**

Step 4: Click on the **More** tab and select **Risks**

Step 5: Click the **Add Risk** button in the middle of the screen

Step 6: **Check the box** on the left for the **risk you created** earlier

Step 7: Click the **Link to Incident** button on the bottom right

Glossary

A

Assessment – A list of questions assigned to a respondent within the OneTrust tool that requires a response by the respondent(s) and subsequent approval by an assigned approver(s)

Asset – Anything that can store or process personal data. This can include an application, website, database, or even physical storage. In GRC, this can also be defined as an item of value to a business

Audit – An official inspection and independent review of information within an organization conducted with a view to express an opinion thereon

B

Breach Response Plan - provides guidelines for organizations to follow each time a breach is discovered. It is the employment of specific recording of the incident, assignments of directly responsible individuals, and use of process workflows for use in responding to an incident

C

Controller – The entity that determines the purposes, conditions, and means of the processing of personal data

Controls – They are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets

Controls Library - Includes controls from recognized frameworks and custom controls that your organization can use to evaluate and describe the security and privacy requirements you have within the OneTrust application

Compliance - the act of ensuring your company and employees follow the laws, regulations, standards, and ethical practices that apply to your organization

Cloud Security Alliance (CSA) - an industry organization dedicated to helping ensure a secure cloud computing environment – founded in 2009

CSA Cloud Controls Matrix (CCM) - a cybersecurity control framework for cloud computing, composed of 133 control objectives that are structured in 16 domains covering all key aspects of the cloud technology

D

Data Element – Pieces of collected information that together, build a complete look at Data

Data Subject – A natural person whose personal data is processed by a controller or processor

E

Encrypted Data – Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Entity – A registered business involved in and responsible for data processing

F

Finding – An issue and/or compliance gap identified by an auditor through an audit work paper

Fed RAMP – The Federal Risk and Authorization Management Program - A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The governing bodies of Fed Ramp include: JAB, OMB, CIO Council, FedRAMP PIO, DHS, and NIST

G

General Data Protection Regulation (GDPR) – A regulation on data protection and privacy for all residents of the European Economic Area. Passed in 2016, in effect in 2018

Governance - the way rules, norms & actions are structured, sustained, regulated, and held accountable

I

ISO 27001 - International Organization for Standardization (ISO) 27001 - formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). Issued and maintained by International Organization for Standardization.

ISO 29001 – International Organization for Standardization (ISO) 29001 - ISO 29001 defines the quality management system for product and service supply organizations for the petroleum, petrochemical, and natural gas industries

IT Risk Management - The set of Policies, Procedures, as well as the technology that an organization puts into place to reduce threats, vulnerabilities, and other results caused by having unprotected data

N

NIST 800-171 - The National Institute of Standards and Technology - The NIST Special Publication 800-171 governs Controlled Unclassified Information (CUI) in Non-Federal Information Systems and Organizations

P

Policy – Clarifies expected output & behavior of an organization's members in the context specific to that organization (groups can include employees, volunteers, and other members (board members, etc.)

Processing Activity – An activity where data is touched stored or moved

R

Risk - is defined as the possibility or chance of loss, adverse effect(s), danger, or injury

Risk Register – A central list that includes all risks created within a variety of portions of the OneTrust tool

S

Security Standards/Framework - A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment

T

Template – A list of questions pre-populated in the OneTrust tool that can be created or modified and assigned to someone as an assessment

Threat - Anything that can exploit a vulnerability, either intentionally or accidentally and obtain damage or destroy an asset

V

Vendor – A third-party service provider

Vendorpedia Exchange – a library of vendors within the OneTrust tool that contains detailed security and privacy profiles of thousands of global vendors. Each profile provides extensive information on the vendor details, services, and related certificates

Vulnerability – Defined as weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset

W

Workpaper – Workpapers provide auditors a central location to manage audit work for compliance control. Auditors can access existing evidence, assessments, and control implementations to build their view of a control's effectiveness