OneTrust

PRIVACY, SECURITY, AND GOVERNANCE

GRC Professional Certification Handbook

CERTIFICATION PROGRAM
Professional Track

The training environment provided to you is only for use during the OneTrust Certification Training Program. You will only have access to login in for the duration of training.

Training URL: training.onetrust.com

Please refer to your instructor for the password to your environment.

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.

Error! Unknown document property name.

OneTrust
PRIVACY, SECURITY & THIRD-PARTY RISK

One Trust GRC Certification Program Reference Guide

Prepared For:
OneTrust GRC Professional Certification Attendees
Version 5.0

Introduction

Welcome to the OneTrust GRC 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.

Table of Contents

1 – Frameworks Overview____ 3 – 6

2 – IT Risk Management____ 7 – 14

3 – Inventory & Assessment Automation______________________________ 15 – 20

4 – Vendor Management____ 20 – 26

5 – Enterprise Policy Management____ 26 – 30

6 – Incident Response Management____ 30 – 34

7 – Whistleblower & Ethics Case Management__________________________________ 35 – 38

8 – Audit Management____ 39 – 43

9 – Exam Review____ 43

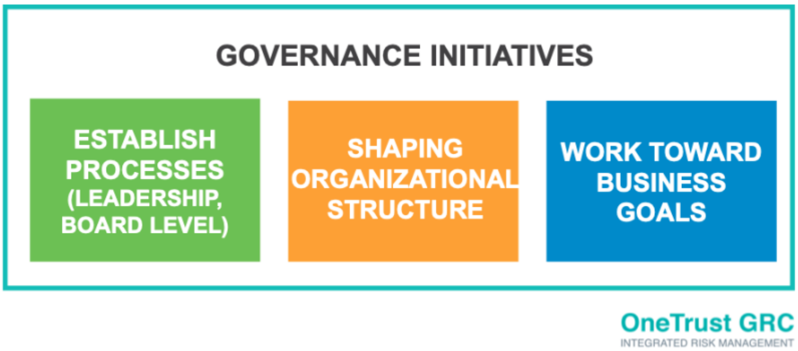
10 – Glossary____ 43 – 46

Error! Unknown document property name.

Terminology & Frameworks Overview

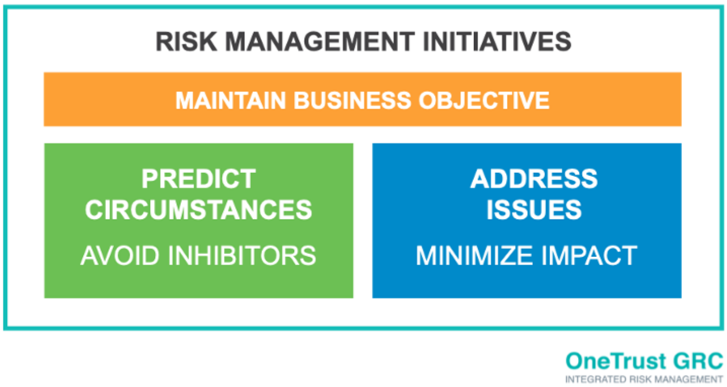
1. Governance

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


GOVERNANCE INITIATIVES
ESTABLISH PROCESSES (LEADERSHIP, BOARD LEVEL)
SHAPING ORGANIZATIONAL STRUCTURE
WORK TOWARD BUSINESS GOALS
OneTrust GRC
INTEGRATED RISK MANAGEMENT

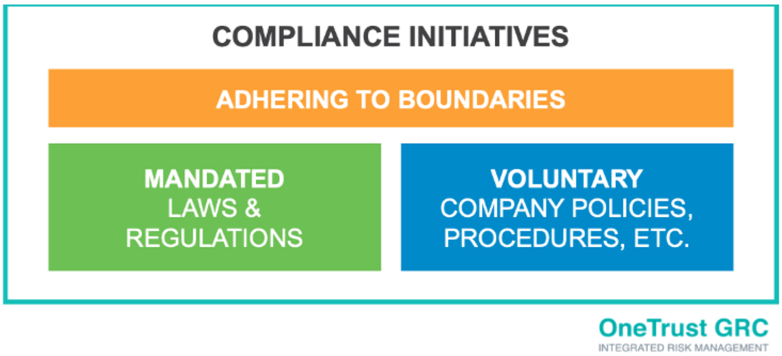
2. Risk

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


RISK MANAGEMENT INITIATIVES
MAINTAIN BUSINESS OBJECTIVE
PREDICT CIRCUMSTANCES
AVOID INHIBITORS
ADDRESS ISSUES
MINIMIZE IMPACT
OneTrust GRC
INTEGRATED RISK MANAGEMENT

3. 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
ADHERING TO BOUNDARIES
MANDATED LAWS & REGULATIONS
VOLUNTARY COMPANY POLICIES, PROCEDURES, ETC.
OneTrust GRC
INTEGRATED RISK MANAGEMENT

Some of the most commonly used frameworks you will find in the controls library:

1. GAPP - **Generally Accepted Privacy Principles**

A framework intended to assist Chartered Accountants and Certified Public Accountants in creating an effective privacy program for managing and preventing privacy risks.

The framework was developed through joint consultation between the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA).

2. CSA CCM - **CSA Cloud Controls Matrix**

The Cloud Security Alliance (CSA) was founded in 2009 and is an industry organization dedicated to helping "ensure a secure cloud computing environment."

The CSA Cloud Controls Matrix (CCM) is 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.

The controls in the CCM are mapped against industry-accepted security standards, regulations, and control frameworks.

3. 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.

4. ISO 27001 - **International Organization for Standardization (ISO) 27001**

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.

5. 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.

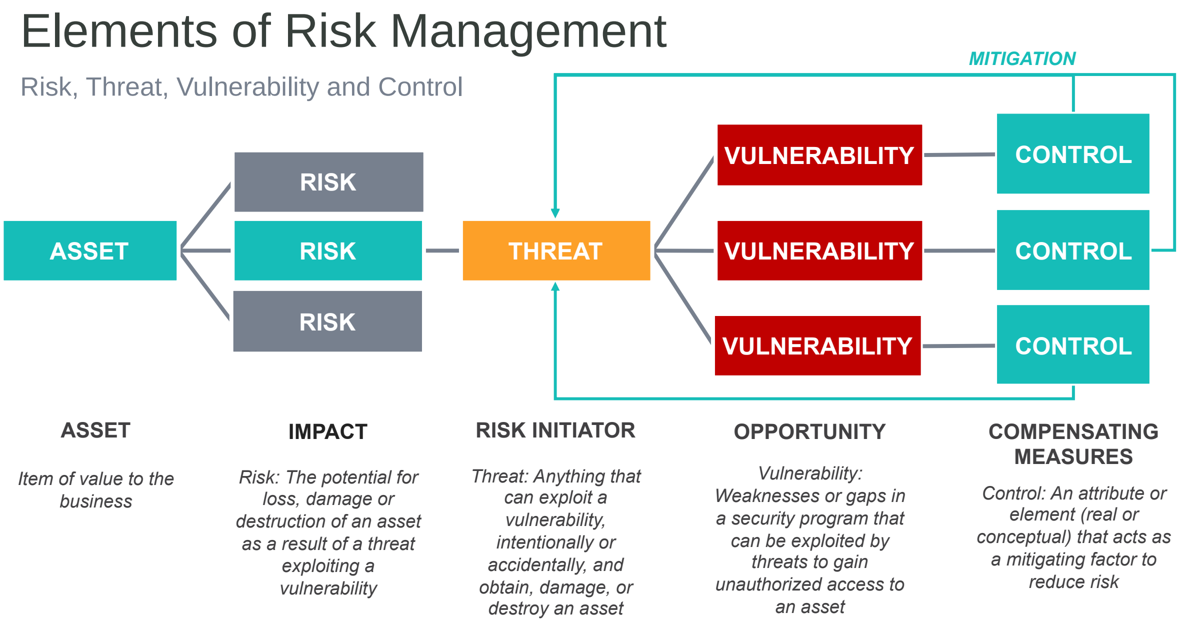
6. NIST 800-171 - **The National Institute of Standards and Technology**

The NIST Special Publication 800-171 governs Controlled Unclassified Information (CUI) in Non-Federal Information Systems and Organizations.

IT Risk Management

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 in order to apply mitigating measures towards those risks.

Module Overview



Elements of Risk Management

Risk, Threat, Vulnerability and Control

ASSET

Item of value to the business

IMPACT

Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability

RISK INITIATOR

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

OPPORTUNITY

Vulnerability: Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset

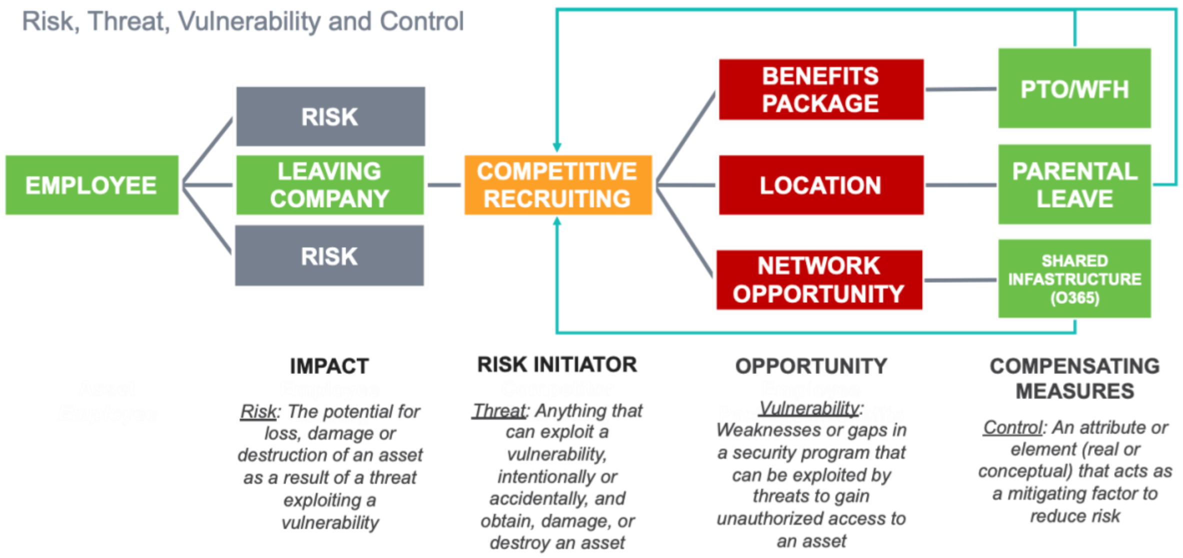
COMPENSATING MEASURES

Control: An attribute or element (real or conceptual) that acts as a mitigating factor to reduce risk

- An **ASSET** is an item of value to your business.
- A **RISK** is the potential for loss, damage, or destruction of an asset as a result of threat exploiting a vulnerability.
- A **THREAT** is anything that can exploit a vulnerability, either intentionally or accidentally and obtain damage or destroy an asset.
- **VULNERABILITIES** can be defined as weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

- A **CONTROL** can be defined as an attribute or element (either real or conceptual) that acts as a mitigating factor to reduce risk.

EXAMPLE of the Elements of Risk Management:



Risk, Threat, Vulnerability and Control

EMPLOYEE

RISK
LEAVING COMPANY
RISK

COMPETITIVE RECRUITING

BENEFITS PACKAGE
LOCATION
NETWORK OPPORTUNITY

PTO/WFH
PARENTAL LEAVE
SHARED INFASTRUCTURE (O365)

IMPACT

Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability

RISK INITIATOR

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

OPPORTUNITY

Vulnerability: Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset

COMPENSATING MEASURES

Control: An attribute or element (real or conceptual) that acts as a mitigating factor to reduce risk

Operational Best Practices

Identify Risk

- Identification of Risks can be done in the system either manually or automatically based on rule logic and how respondents answer your assessments.
- Risk Controls can be imported into the system from specific standards or frameworks

Centralize Risk Register

- While Risks input can result from different actions or rules within the system, the OneTrust Tool offers a centralized risk register that lists all risks added, their source, and also the ability to add a risk directly from within the register.

Monitor performance

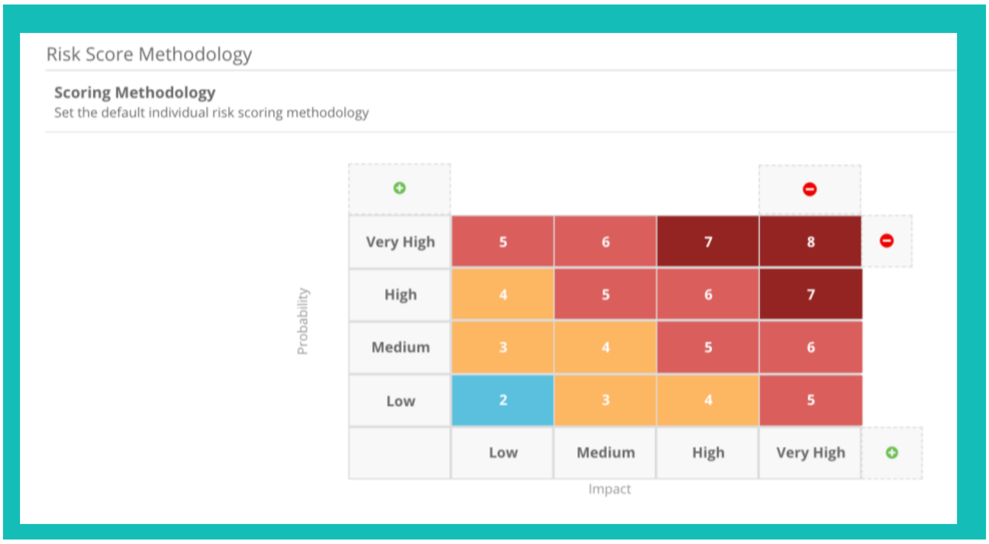
- The Risk Life Cycle and workflow offer a clear monitoring process in order to make sure risk mitigation efforts are working and effective.

- In addition to the role-based risk workflow, automation rules for risks and additional assessments are available via time triggers, risk count, and other measures that can be set up in the system.

Execution in One Trust

1. Configure Risk Score Methodology

OneTrust GRC includes multiple risk scoring methods and also methods for aggregation that you can change depending on what Items in your inventory you are tracking such as Assets, Processing Activities, Vendors, and Entities.



Risk Score Methodology

Scoring Methodology

Set the default individual risk scoring methodology

Probability

	Low	Medium	High	Very High
Very High	5	6	7	8
High	4	5	6	7
Medium	3	4	5	6
Low	2	3	4	5

Impact

Step 1: Click the “Launch Pad” (grid icon) at the top left of the screen

Step 2: Click on the IT Risk Management Module (second column, top result)

Step 3: On the Menu that appears on the left, scroll down to the bottom left and click the settings tab

Step 4: On the middle right of the screen, click on the Scoring Methodology dropdown and choose either Matrix or Standard. (if you choose Standard, the next steps are not necessary)

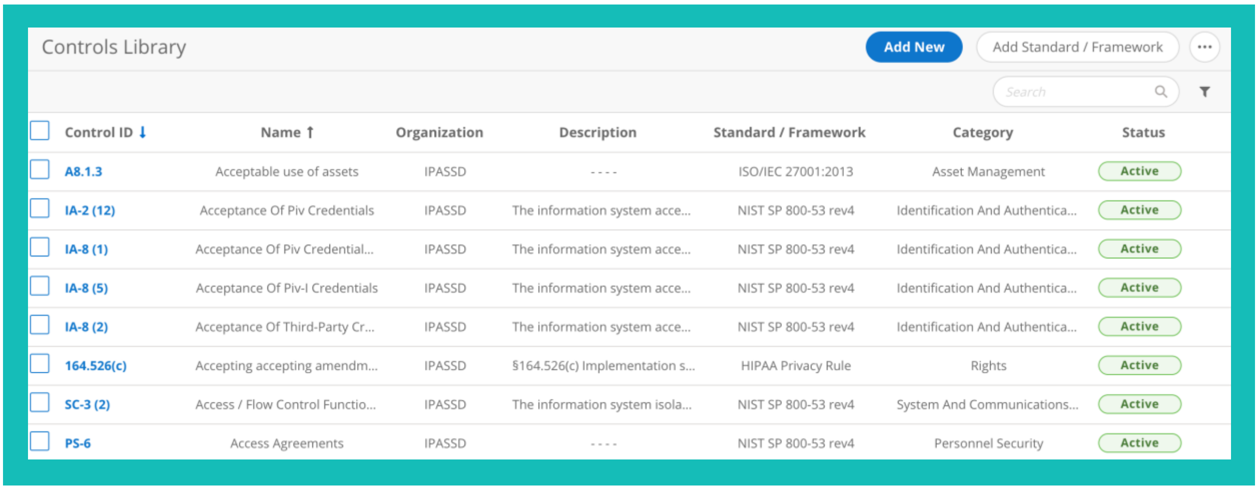
Step 5: If you chose Matrix, go to the bottom left corner of the matrix, edit that block and change “2” to “1”

Step 6: Scroll down to the Risk Level Ranges bar and then drag the yellow category marker over the marker for 2.

Step 7: Click the Blue Save Button at the bottom right of the screen

2. Import controls from standards / frameworks

The OneTrust Tool provides users with a **Controls Library** with the ability to add controls **FROM** multiple standards/frameworks or from scratch to be added **TO** inventory items such as your Assets, Processing Activities, Vendors, Entities, and Risks themselves



□	Control ID ↓	Name ↑	Organization	Description	Standard / Framework	Category	Status
□	A8.1.3	Acceptable use of assets	IPASSD	- - - -	ISO/IEC 27001:2013	Asset Management	Active
□	IA-2 (12)	Acceptance Of Piv Credentials	IPASSD	The information system acce...	NIST SP 800-53 rev4	Identification And Authentica...	Active
□	IA-8 (1)	Acceptance Of Piv Credential...	IPASSD	The information system acce...	NIST SP 800-53 rev4	Identification And Authentica...	Active
□	IA-8 (5)	Acceptance Of Piv-I Credentials	IPASSD	The information system acce...	NIST SP 800-53 rev4	Identification And Authentica...	Active
□	IA-8 (2)	Acceptance Of Third-Party Cr...	IPASSD	The information system acce...	NIST SP 800-53 rev4	Identification And Authentica...	Active
□	164.526(c)	Accepting accepting amendm...	IPASSD	§164.526(c) Implementation s...	HIPAA Privacy Rule	Rights	Active
□	SC-3 (2)	Access / Flow Control Functio...	IPASSD	The information system isola...	NIST SP 800-53 rev4	System And Communications...	Active
□	PS-6	Access Agreements	IPASSD	- - - -	NIST SP 800-53 rev4	Personnel Security	Active

Step 1: Click the “Launch Pad” (grid icon) at the top left of the screen

Step 2: Click on the IT Risk Management Module (second column, top result)

Step 3: Click the Setup Tab on the left side of the screen

Step 4: Then Click the Controls Library Tab on the left side of the screen

Step 5: Click the blue Add New Button at the Top Right of the Screen

Step 6: for “Control ID,” type in “A.8 2.5”

Step 7: for “Name” type in Consultant Two Factor Access

Step 8: for “Status” dropdown, select Active

Step 9: for “standard/framework” dropdown, select ISO/IEC 27001:2013

Step 10: Click the Blue Save button at the bottom right of the menu

Step 11: Click the White Add Standard/Framework Button at the top right of the screen

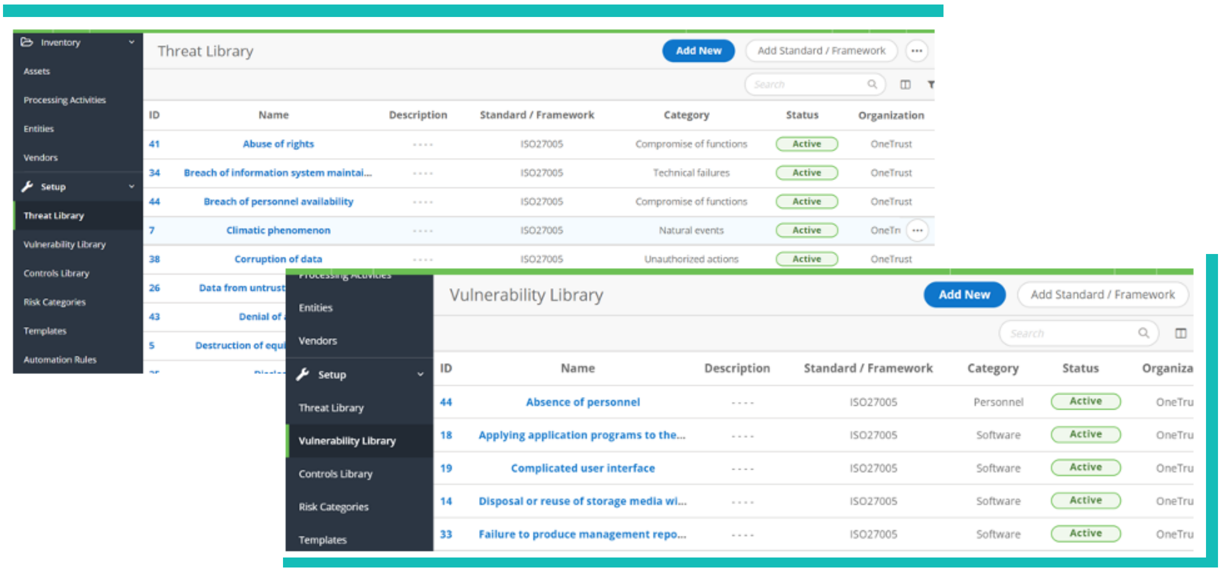
Step 12: Scroll to the bottom of the Standard/Framework list

Step 13: Click on “NIST Cybersecurity Framework Core v1.1

Step 14: Click the Blue Add Button at the bottom right of the menu

2. Add Threats and Vulnerabilities

In the same way we documented our controls, we can document both threats and vulnerabilities within the OneTrust Threat and Vulnerability Library.



Threat Library

ID	Name	Description	Standard / Framework	Category	Status	Organization
41	Abuse of rights	- - - -	ISO27005	Compromise of functions	Active	OneTrust
34	Breach of information system maintai...	- - - -	ISO27005	Technical failures	Active	OneTrust
44	Breach of personnel availability	- - - -	ISO27005	Compromise of functions	Active	OneTrust
7	Climatic phenomenon	- - - -	ISO27005	Natural events	Active	OneTr
38	Corruption of data	- - - -	ISO27005	Unauthorized actions	Active	OneTrust
26	Data from untrust					
43	Denial of					
5	Destruction of equi					

Vulnerability Library

ID	Name	Description	Standard / Framework	Category	Status	Organiza
44	Absence of personnel	- - - -	ISO27005	Personnel	Active	OneTru
18	Applying application programs to the...	- - - -	ISO27005	Software	Active	OneTru
19	Complicated user interface	- - - -	ISO27005	Software	Active	OneTru
14	Disposal or reuse of storage media wi...	- - - -	ISO27005	Software	Active	OneTru
33	Failure to produce management repo...	- - - -	ISO27005	Software	Active	OneTru

Step 1: Go to the Setup Tab area on the left side of the screen

Step 2: Click on the Threat Library Tab on the middle left of the screen

Step 3: Click the White Add Standard/Framework Button at the top right of the screen

Step 4: Click the box for ISO27005

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

Step 6: Click the Blue Add New button at the top right of the screen

Step 7: For “Threat ID” enter 99

Step 8: For “Threat Name” enter Data Loss

Step 9: For “Category” dropdown, select Data Minimalization and Retention

Step 10: Click the Blue Add Button at the bottom right of the menu

Step 11: Go to the Setup Tab Area on the left side of the screen

Step 12: Click on the Vulnerability Library Tab on the middle left of the screen

Step 13: Click the White Add Standard/Framework Button at the top right of the screen

Step 14: Click the box for ISO27005

Step 15: Click the blue Add button at the bottom right side of the menu

Step 16: Click the Blue Add New button at the top right of the screen

Step 17: For “Vulnerability ID” enter 101

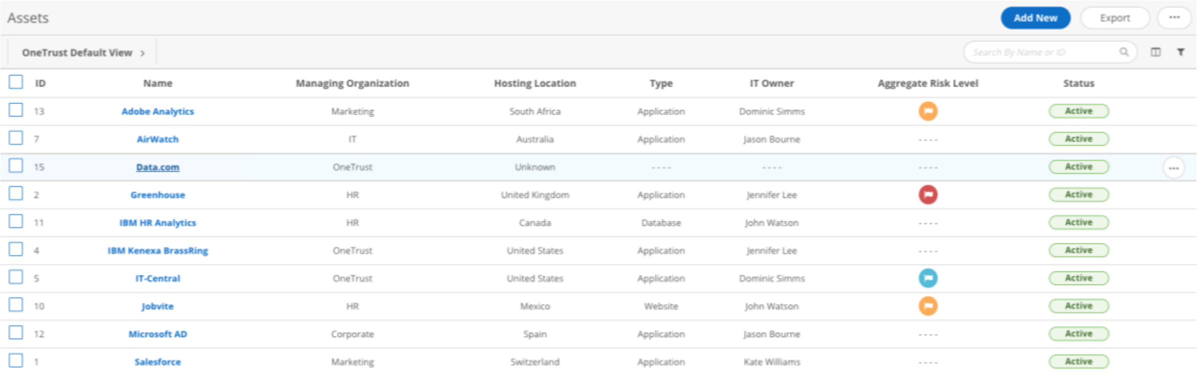
Step 18: For “Vulnerability Name” enter CBC Decryption

Step 19: For “Category” dropdown, select Compromise of Information

Step 20: Click the blue Add button at the bottom right side of the menu

2. Add an Asset

While there are multiple ways to add assets to your inventory, in this exercise, we’ll use the manual interface. The OneTrust tool gives our customers the ability not only to add and track assets within our inventory, but to do the same for Processing Activities, Entities, and Vendors as well.



□ ID	Name	Managing Organization	Hosting Location	Type	IT Owner	Aggregate Risk Level	Status
□ 13	Adobe Analytics	Marketing	South Africa	Application	Dominic Simms	●	Active
□ 7	AirWatch	IT	Australia	Application	Jason Bourne	----	Active
□ 15	Data.com	OneTrust	Unknown	----	----	----	Active
□ 2	Greenhouse	HR	United Kingdom	Application	Jennifer Lee	●	Active
□ 11	IBM HR Analytics	HR	Canada	Database	John Watson	----	Active
□ 4	IBM Kenexa BrassRing	OneTrust	United States	Application	Jennifer Lee	----	Active
□ 5	IT-Central	OneTrust	United States	Application	Dominic Simms	●	Active
□ 10	Jobvite	HR	Mexico	Website	John Watson	●	Active
□ 12	Microsoft AD	Corporate	Spain	Application	Jason Bourne	----	Active
□ 1	Salesforce	Marketing	Switzerland	Application	Kate Williams	----	Active

Step 1: Click the Assets Tab on the left side of the screen under Inventory

Step 2: Click the Blue Add new Button at the top right of the screen

Step 3: For “Name,” enter Payroll Database

Step 4: For “Managing Organization” dropdown, select OneTrust

Step 5: For “Hosting Location” dropdown, select United Kingdom

Step 6: For “Type,” select Database

Step 7: Click the Blue Save Button at the bottom right of the menu

Step 8: Click on the Risks tab at the top of the middle of the screen

Step 9: Click the Blue Add Risk button in the middle of the screen

Step 10: Select an inherent Risk Level

Step 11: For “Threat,” Choose the one you created earlier, or another threat of your choice

Step 12: For “Vulnerability,” Choose the one you created earlier, or another threat of your choice

Step 13: for “Category,” select security

Step 14: Assign a risk owner

Step 15: Assign a risk approver

Step 16: for Description, add “Compromise of information and risk of losing payroll transaction information.”

Step 17: Click the Save and add controls button.

Step 18: On bottom left of the Standard/Frameworks menu, click Nist Cybersecurity Framework.

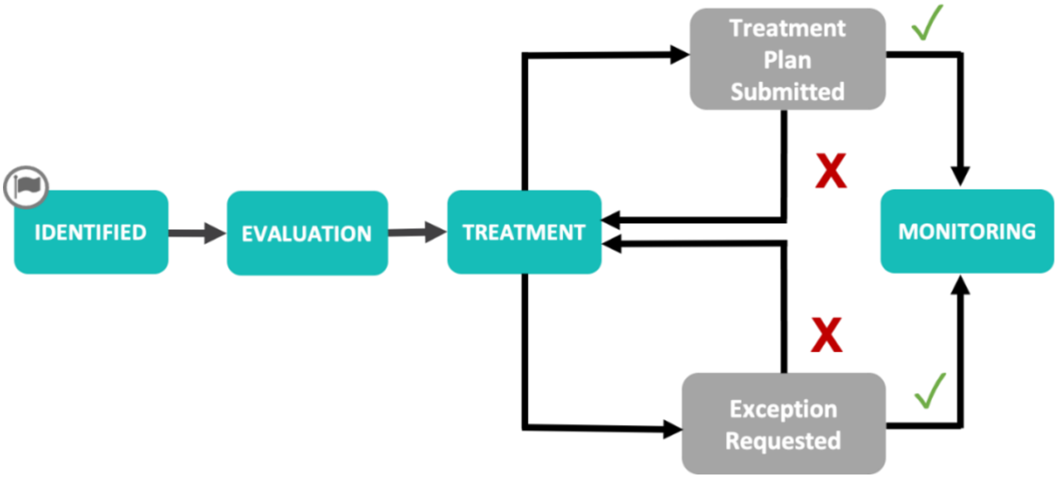
Step 19: At the top right of the menu, type “backup” into the search bar.

Step 20: Check the box for the “PR.IP-4 Backups of information…”

Step 21: Click the Add button

3. Manage risks

Risk Lifecycle: Whether identified automatically by logic/risk rules, or triggered manually as we saw in the last exercise, Risks have a 4 stage lifecycle.

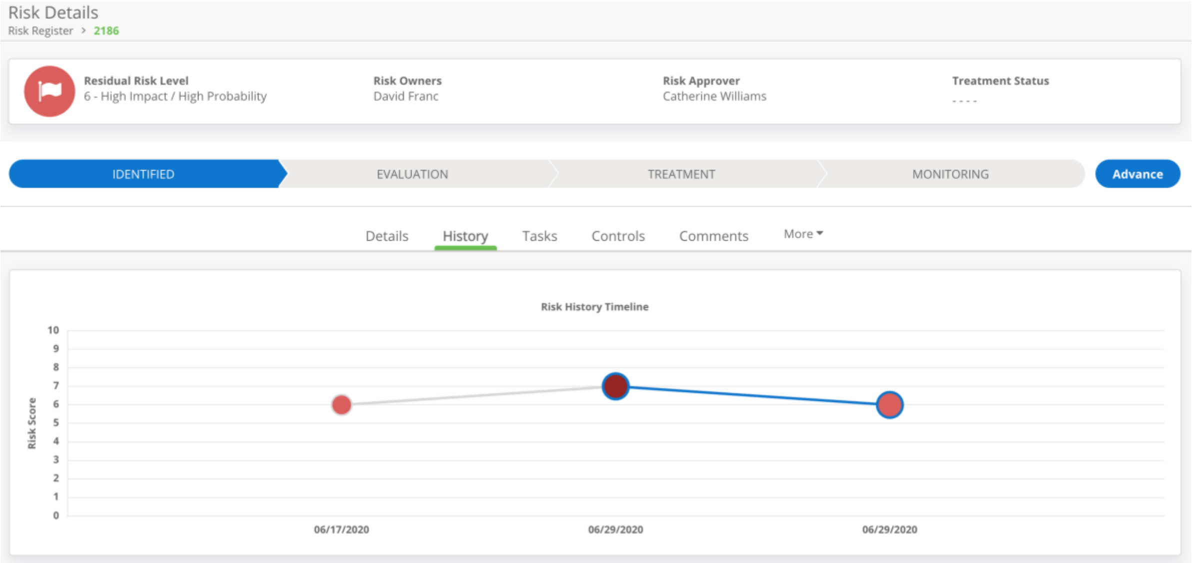


Identified – The risk description is added and also can be further identified via categories, associated threats and vulnerabilities, and an inherent risk level

Evaluation – Evaluation reports can be submitted into the system and the risk owner is identified (directly responsible individual)

Treatment – The Risk Approver submits a treatment recommendation and the assigned risk owner will either submit a treatment plan that aligns with the recommendation or they will request an exception.

Monitoring – During the final phase, risk history can be observed as well as the addition of a residual risk level resulting from the mitigation of the risk.



Risk Details

Risk Register > 2186

Residual Risk Level: 6 - High Impact / High Probability

Risk Owners: David Franc

Risk Approver: Catherine Williams

Treatment Status: ----

Step 1: Click the ID number for the risk you just added

Step 2: Advance your risk to the Treatment phase by clicking on the Treatment stage.

Step 3: Assign yourself as risk owner

Step 4: Enter a treatment plan

Step 6: Click the save and advance button

Step 7: At the top right of the screen, click the white Request Exception button.

Step 8: For comments, enter “Encryption Systems with CBC Countermeasures already engaged”

Step 9: Click the blue submit button

Step 10: Click the Blue Grant Exception button at the top right of the screen menu.

Step 11: for Result, select “Avoided”

Step 12: Change your residual risk score

Step 13: Click the Blue Confirm Button

Inventory & Assessment Automation

In this module we focus on using GRC Assessments to obtain information about our assets and other inventory items, deliver them to the correct respondents, and how to automate periodic updates to save time and reduce unnecessary extra work.

Module 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 evidences
- Explain

Regulation Example:

ISO 27001: the international standard that describes best practice 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 likelihood of these scenarios happening

Operational Best Practices

Use Dynamic Question Types

- OneTrust has configured question types specifically designed to sync the answers with your inventory items, attributes, and your controls as well.

Save Time With Logic

- OneTrust tool uses Automation, Skip, and Rule logic which can be used to create risks, send additional assessments, skip certain questions for the respondent, among other actions.

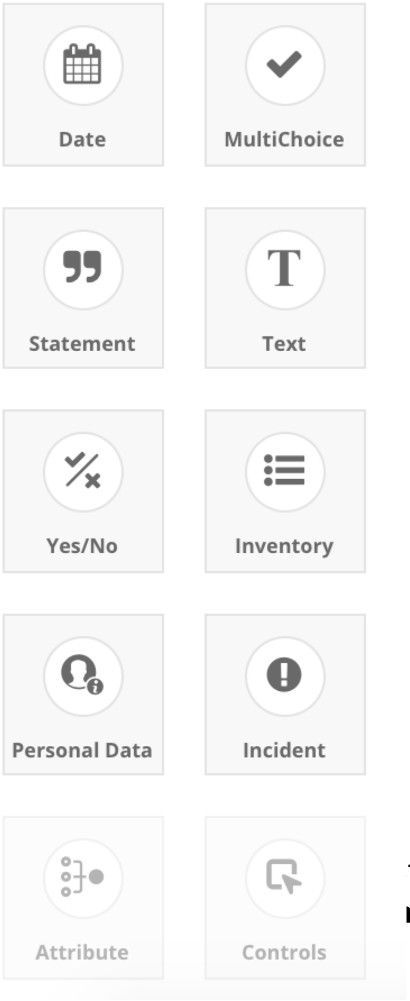
Create your own Dashboards

- Progress can be tracked at a higher visual level for status checks using Dashboards which can also be modified to suit and organization's needs.

Execution in One Trust

1. Creating a dynamic template from scratch

- A Template is a list of pre-populated questions within the OneTrust Tool. This template becomes an assessment when it is launched and assigned to someone
- Templates can be built from scratch or OneTrust's pre-built templates cam be used unaltered or modified to fit your company's specific needs.



Step 1: Click on the Launch Pad at the top left of the screen and then click IT Risk Management

Step 2: Click Setup and then click Templates at the bottom left of the screen

Step 3: Click the View Button for the ITRM Templates box in the center of the screen

Step 4: Click the white create custom template button at the top right of the screen

Step 5: For "Name," enter Asset Review Template

Step 6: Click the Blue Create Template button at the bottom right of the menu

Step 7: Click the Blue Add Section Button at the center of the screen

Step 8: For "Section Name," enter Asset Information

Step 9: Click the Blue Add Section Button

Step 10: On the lower left sid

Step 10: on the lower left side of the screen click and drag the inventory block under section

Step 11: under question configuration on the top left of the menu, select "assets" in the inventory dropdown.

Step 12: For "Question," enter "what is the name of this asset?

Step 13: For Friendly Name, enter 'Asset Name"

Step 14: Click the blue save button at the bottom right of the screen

Step 15: Click and drag the Attribute Block from the bottom left of the screen and drop it just below question 1.1 "Asset Name"

Step 16: For the question "Which Inventory record should this update" select 1.1 asset name

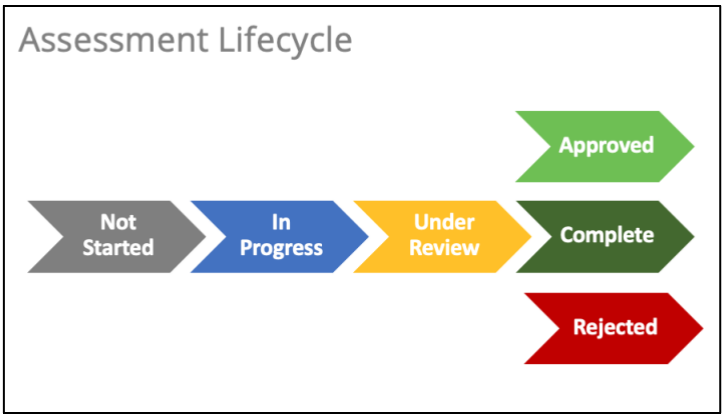
Step 17: For the question Which Attribute? Select type

Step 18: Repeat steps 1 & 2 above and select an additional attribute.

Step 19: Click the save button at the bottom right of the menu

Step 20: Click the publish button at the top right of the screen

Step 21: Click Confirm



Not Started – Assessment is assigned and respondent receives an assessment notification.

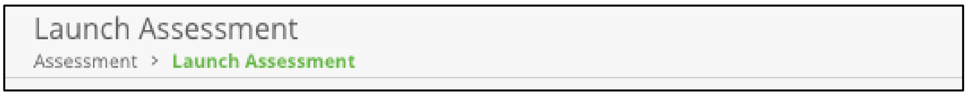
In Progress – Respondent begins to answer questions and submits assessment for approval.

Under Review – Approver can send questions back, make comments, ask questions, assign risks, and finish review.

Complete – Once Assessment is complete, it must be labelled as approved or rejected by the approver.

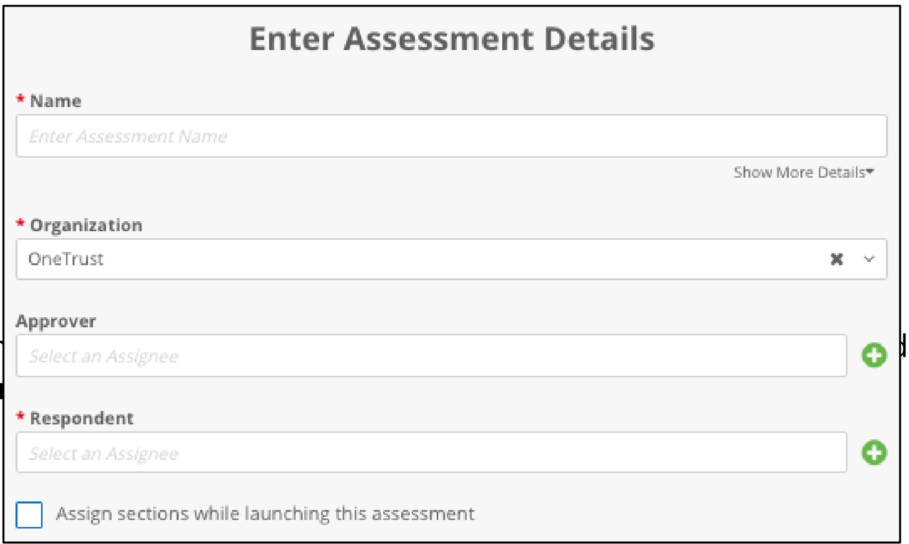
2. Sending and Assessment

- Assessments do not have to have the same name as their source template.
- Assessments can be used with respondents in the systems or for external respondents such as vendors or contractors.
- Assessments can be launched multiple ways, including from the assessment menu, directly from the inventory, or through automated/logic rules.



Launch Assessment

Assessment > Launch Assessment



Enter Assessment Details

* Name

Enter Assessment Name

Show More Details

* Organization

OneTrust

Approver

Select an Assignee

* Respondent

Select an Assignee

□ Assign sections while launching this assessment

Step 1: Click on the Assessments tab on the top left of screen

Step 2: Click the blue 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 Approver, assign yourself

Step 7: For Respondent, select a name from the respondent dropdown

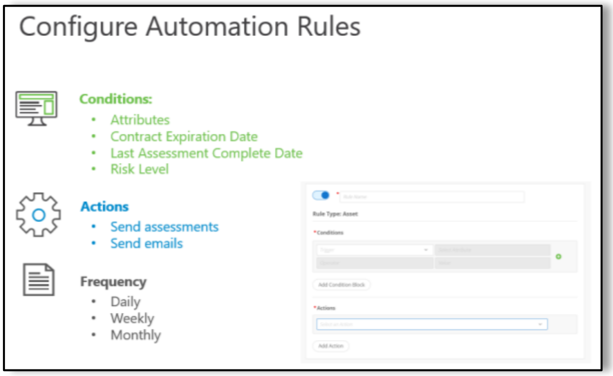
Step 8: Click the Green Plus Button next to respondent field

Step 9: Select an additional respondent

Step 10: Click the Blue Launch Button at the bottom right of the screen

3. Create automation rules

- If we need to periodically ask questions and review details or send notifications on Inventory and other items such as contracts, this is something we can pre-set the system to do for us, rather than have to remember or possibly forget to do.



Configure Automation Rules

Conditions:

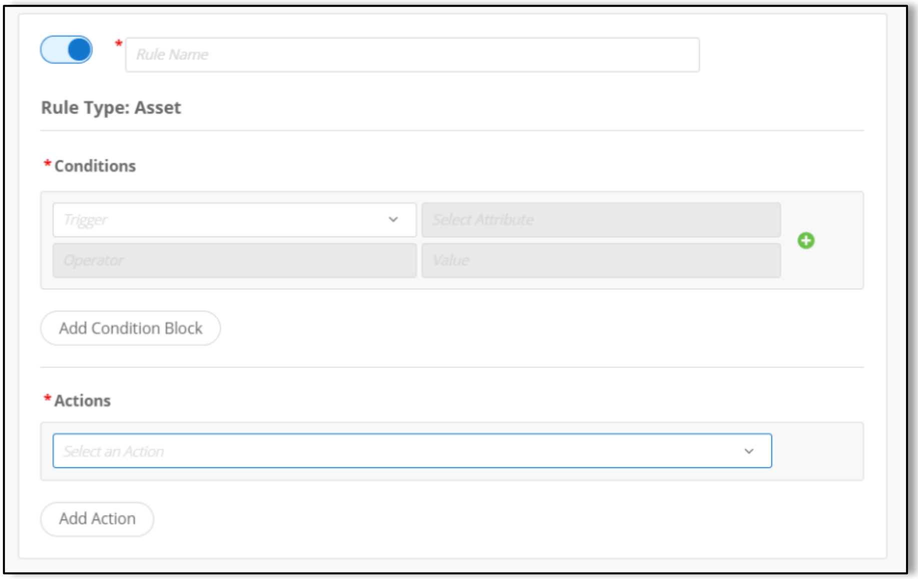
- Attributes
- Contract Expiration Date
- Last Assessment Complete Date
- Risk Level

Actions

- Send assessments
- Send emails

Frequency

- Daily
- Weekly
- Monthly



Rule Type: Asset

Step 1: Click the Automation Rules tab at the bottom left of the screen

Step 2: Click the Blue 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 Blue Add button at the bottom right of the menu

Step 6: Click the Blue Add Rule button at the center of the screen

Step 7: For Select a Rule Type dropdown, select Asset

Step 8: Click the blue Continue Button

Step 9: For Rule Name, type in “Asset Review Rule”

Step 10: For Trigger dropdown, select “Last Assessment Completion Date – By Template.”

Step 11: For Operator dropdown, select “Equal To.”

Step 12: For Number, enter 180

Step 13: For Select a Template, click on the field and choose the Asset Review Template you choose earlier

Step 14: For Actions Dropdown, select “Send Asset Assessment.”

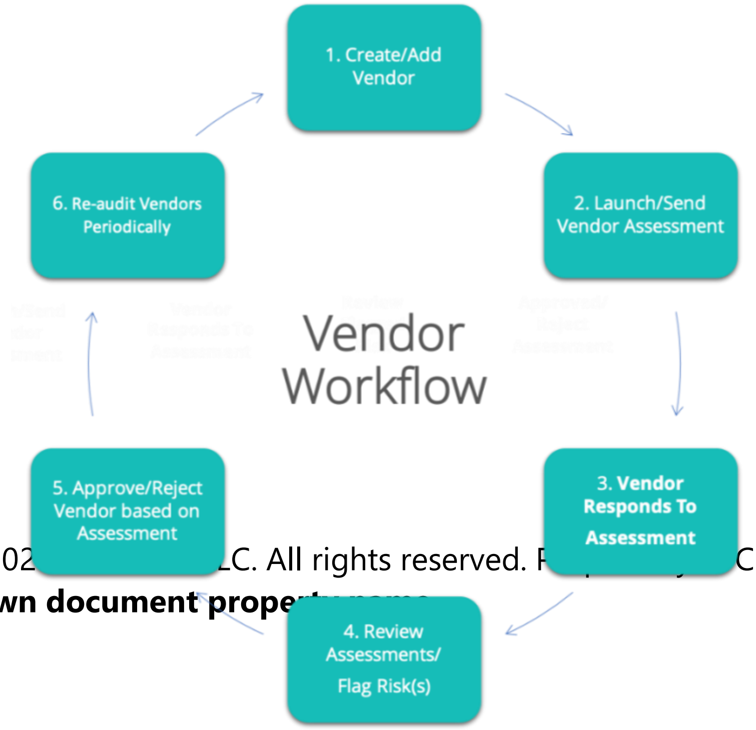
Step 15: For Template Name, click on the field and select the asset review template you created earlier

Step 16: Add optional approvers and respondents if you would like, then click the Blue Save button at the bottom right of the screen.

Vendor Risk Management

While business relationships with third party vendors can often align with your organization’s goals, it unfortunately also has the potential to lead to similar types of threats, vulnerabilities, and risks that we discussed in prior modules. In this module covers overview, best practice, and practical steps in the OneTrust Tool to help organizations in efforts to manage these factors.

Module Overview


1. Create/Add Vendor
2. Launch/Send Vendor Assessment
3. Vendor Responds To Assessment
4. Review Assessments/ Flag Risk(s)
5. Approve/Reject Vendor based on Assessment
6. Re-audit Vendors Periodically
Vendor Workflow

Operational Best Practices

Vendor Templates

- OneTrust’s pre-built templates are already configured to be used to assess vendors against a number of existing and common frameworks and standards.
- These can be set up to be used as is, or you can modify them particular to your organization’s needs.
- We can also set up rules to automatically send notifications, assessments, or even assign risks based on how questions are answered and use skip logic to save time on getting answers from vendors.

Periodically Monitor Vendors

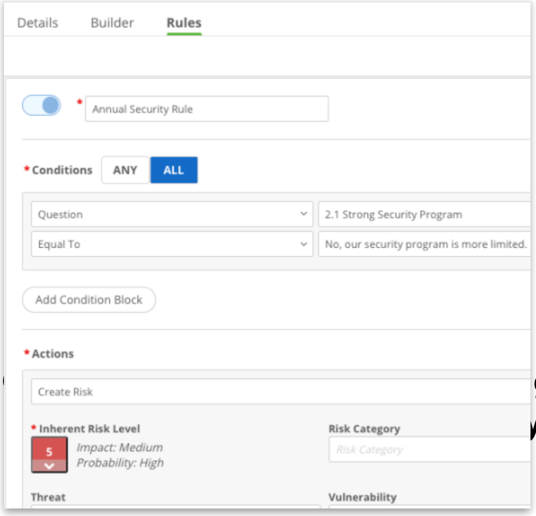
- The system can be set to periodically monitor vendors to make sure that they meet an organization’s security standards.
- Within the system, rules and frequency triggers can be set up for assessments, contracts, engagements, and other important aspects within the process of vendor evaluation

Onboarding / Offboarding

- Onetrust has default onboarding and offboarding workflows that can be edited to add custom stages, notifications, subtasks, and integrations particular to an organization.
- Engagements, contracts, risks and other items can also be managed within these workflows

Execution in One Trust

1. Create a Rule-Based Template



* Annual Security Rule

* Conditions ANY **ALL**

Question: 2.1 Strong Security Program

Equal To: No, our security program is more limited.

* Actions

Create Risk

* Inherent Risk Level: 5 — *Impact: Medium* *Probability: High*

Risk Category: *Risk Category*

Threat

Vulnerability

Step 1: Click on the Launchpad icon at the top left of the screen

Step 2: Click on Vendor Management

Step 3: Go to the Setup tab area on the lower left side of the screen

Step 4: Click on the Templates Tab on the lower left side of the screen

Step 5: Click the Blue Choose from Gallery Button at the top right of the screen

Step 6: Click into the search bar at the top middle of the screen and type "Vendor Privacy"

Step 7: Click the Vendor Privacy & Security Program Questionnaire Box

Step 8: Click the Blue Choose this Template Button at the bottom right of the screen

Step 9: Type your initials in front of the existing name in the name field

Step 10: Click the Blue Create Template Button

Step 11: Click the Rules Tab at the top middle of the screen

Step 12: Click the White Add Rule Button at the top right of the screen

Step 13: For Rule Name, enter "high risk rule"

Step 14: For Trigger Dropdown, select "question"

Step 15: For Question Dropdown, select 8.6 Access Revocation

Step 16: For Operator Dropdown, select Equal To

Step 17: For Response Dropdown, select No

Step 18: For Select an Action Dropdown, select Create Risk

Step 19: For Inherent Risk Level, Choose a High Risk

Step 20: Click the White Add Risk Control Button at the bottom right of the menu

Step 21: Click on a Standard/Framework from the list on the left side of menu

Step 22: Check the box for the Risk Control you would like to add

Step 23: Click the Blue Add Button at the bottom right of the menu

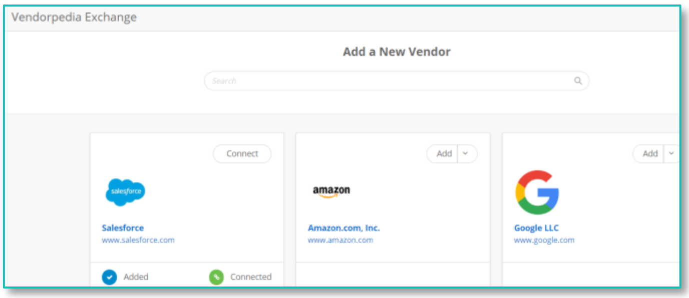
Step 24: Click the Blue Save Button at the bottom right of the screen

Step 25: Click the Blue Publish Button at the top Right of the Screen

Step 26: Click the Blue Confirm Button at the Center of the Screen

2. Add Vendors to Inventory Using Vendorpedia

Vendors can be added into your inventory through the manual interface from scratch, but can also be added using Onetrust's Vendorpedia, a library that includes information including certificates, popular assessments, and more for over 68,000 vendors.



Vendorpedia Exchange

Add a New Vendor

Search

Connect	Add	Add
Salesforce www.salesforce.com	Amazon.com, Inc. www.amazon.com	Google LLC www.google.com
Added Connected		

Step 1: Go to the Vendorpedia tab area on the left side of the screen

Step 2: Click the exchange tab on the left side of the screen

Step 3: Close any popup message that occurs

Step 4: Click on Google

Step 5: Click on the Certificates tab at the top left of the screen

Step 6: Click on G Suite on the top left of the screen

Step 7: Check for an ISO/IEC 27001:2013 Certificate

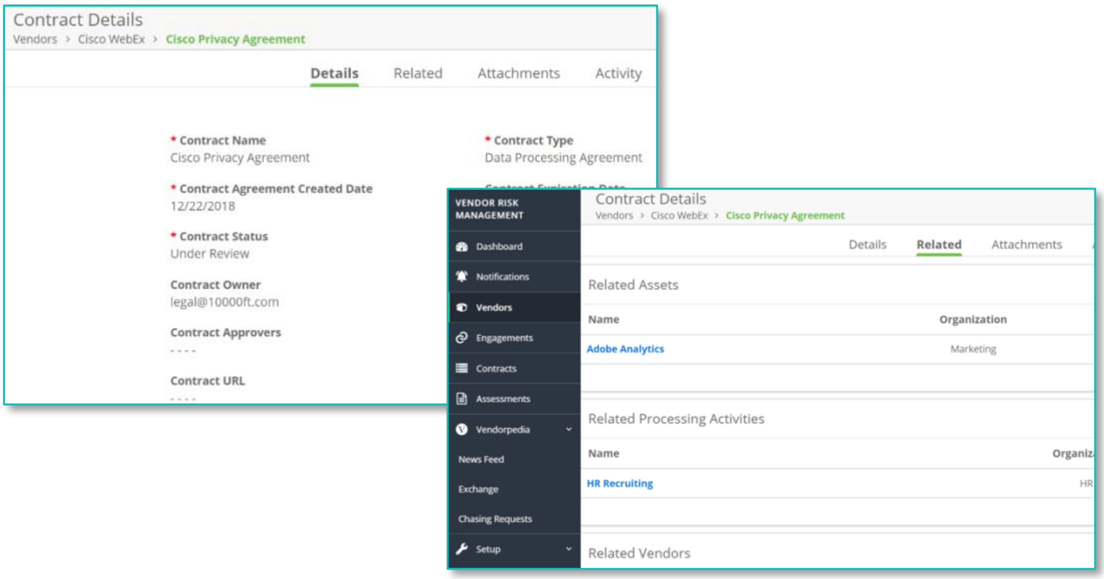
Step 8: Click the White Add button at the top right of the screen

Step 9: Select G-Suite and click the Blue next button at the bottom right of the screen

Step 10: Click the Blue Connect Button at the bottom right of the screen

3. Manage contract records

Contracts, engagements, related risks, threats, vulnerabilities, and more can be manage in the Vendor Inventory. This exercise includes management of a contract within a vendor inventory record.



Contract Details
Vendors › Cisco WebEx › Cisco Privacy Agreement

* Contract Name
Cisco Privacy Agreement

* Contract Type
Data Processing Agreement

* Contract Agreement Created Date
12/22/2018

* Contract Status
Under Review

Contract Owner
legal@10000ft.com

Contract Approvers
- - - -

Contract URL
- - - -

Contract Details
Vendors › Cisco WebEx › Cisco Privacy Agreement

Related Assets

Name	Organization
Adobe Analytics	Marketing

Related Processing Activities

Name	Organiz
HR Recruiting	HR

Related Vendors

Step 1: Click on the Contracts tab at the left side of the screen

Step 2: Click on the Blue Add Contract Button at the top right of the screen

Step 3: For Primary Vendor, Select the vendor you added before, or add Google

Step 4: for Contract Name, Type in your vendor's name and then "MSA Contract"

Step 5: For Contract Type select Master Service Agreement

Step 6: Select a Contract Agreement Created Date

Step 7: Select a Contract Expiration Date

Step 8: For Contract Status Select Signed

Step 9: Click the Blue Add Button at the Bottom Right

Step 10: In the Contract Name Column at the top right, click into the contract you created by clicking the contract name.

Step 11: Click on the Related tab at the top middle of the screen

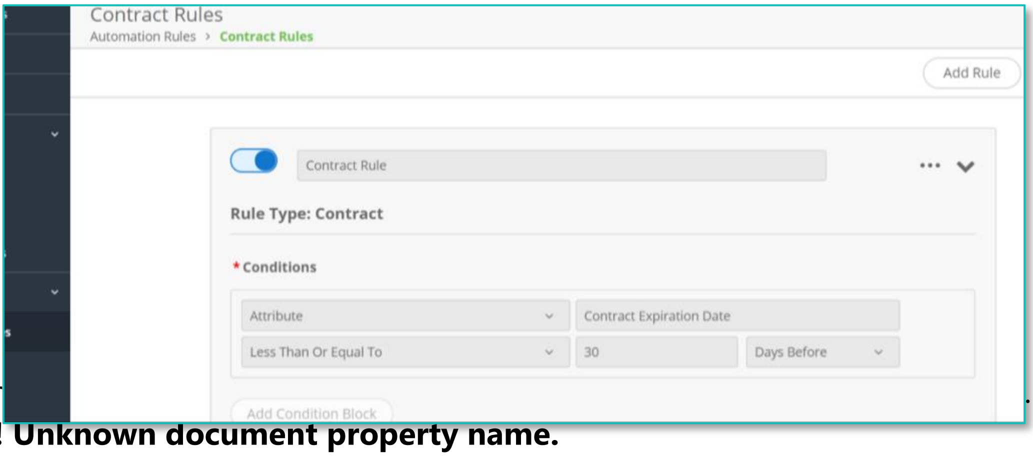
Step 12: Click the Blue Add Related Asset Button in the middle of the screen

Step 13: For the Choose an Asset Dropdown, select an asset

Step 14: Click the Blue Add Related Button at the bottom right of the menu

4. Create automation rules

Automation rules to manage contracts like the one created in the previous exercise. Rules can be created based in attributes for the contract, such as expiration date and days before or after that date. Actions can be triggered by those conditions.



Contract Rules

Automation Rules › Contract Rules

Contract Rule

Rule Type: Contract

* Conditions

Attribute: Contract Expiration Date

Less Than Or Equal To: 30 Days Before

Step 1: Go to the Setup tab area on the lower left side of the screen

Step 2: Click on the Automation Rules Tab

Step 3: Click the Blue Add Rule Group Button At the top Right of the Screen

Step 4: For Rule Group Name, enter Contract Rules

Step 5: For Organization, select OneTrust

Step 6: Click the Blue Add Button at the bottom right of the menu

Step 7: Click the Blue Add Rule Button at the Center of the Screen

Step 8: For Rule Type Dropdown, Select Contract

Step 9: Click the Blue Continue Button

Step 10: For Rule Name, type in Contract Email Rule

Step 11: For Trigger Dropdown, select Attribute

Step 12: For Select Attribute Field, select Contract Expiration Date

Step 13: For Operator, select Equal to

Step 14: For Number Select 30

Step 15: For Action Dropdown, select Send Contract Email

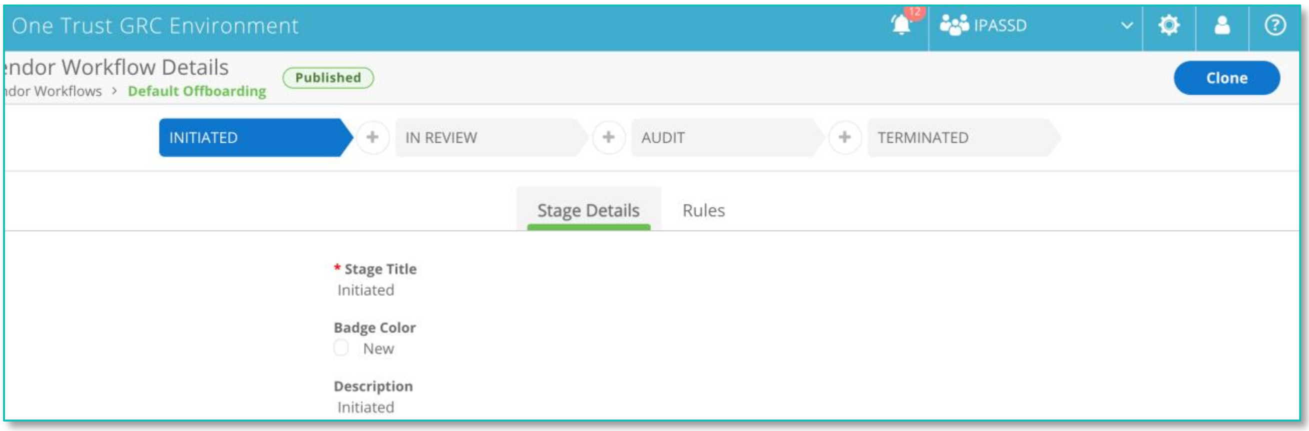
Step 16: For Recipients dropdown, select a recipient

Step 17: For Email Template, select Contract Expiring

Step 18: Click the Blue Save Button at the Bottom Right of the Screen

5. Create Offboarding Workflow

Custom workflows can be created to onboard and offboard vendors with stages and subtasks added that are particular to an organization’s needs.



* Stage Title
Initiated

Badge Color
New

Description
Initiated

Step 1: Go to the Setup tab area on the lower left side of the screen

Step 2: Click on the Workflows Tab on the left side of the screen

Step 3: Click the Blue View Button under Vendor Workflows in the center of the screen

Step 4: Click on the Default Offboarding Workflow

Step 5: Click the Blue Clone Button at the Top Right of the Screen

Step 6: For Workflow Name, type in High Risk Offboarding

Step 7: Click the Blue Clone Button at the bottom right of the menu

Step 8: Click into High Risk Offboarding Workflow

Step 9: At the top middle of the screen, click the plus button between In Review and Audit

Step 10: For Stage Title, enter Data Purge Verification

Step 11: Click the Blue Add Button at the bottom right of the menu

Step 12: Click the Rules Tab at the top middle of the screen

Step 13: Click the Blue Add Rule Button in the center of the screen

Step 14: For Rule Name, enter Data Purge

Step 15: Go down to the Actions dropdown and select "Create Task."

Step 16: For Name, type in Verify all essential data is purged from vendor and backed up onto secure storage

Step 17: Select an assignee

Step 18: Click the blue Save Button at the bottom right of the menu

Step 19: Click the Blue Publish Button at the Top Right of the Screen

Step 20: Click Publish in the center 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 creation of new policies to retiring policies that are no longer needed.

Module Overview

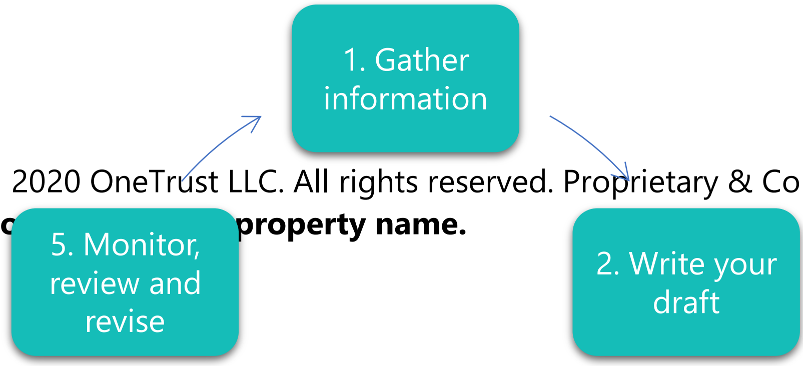
What do policies do?

- Clarify expected output & behaviour 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 for decision making
- Aid in simplification of processes

Ideal Policy Workflow:



Operational Best Practices

Determine policies needed

Three questions to ask when determining necessary policies:

- *Is this a policy that is being created in anticipation of needing it later on?*
- *Or alternatively, is this policy created in response to a need that has come up?*
- *Is this policy internal or external to our organization?*

Clear policies

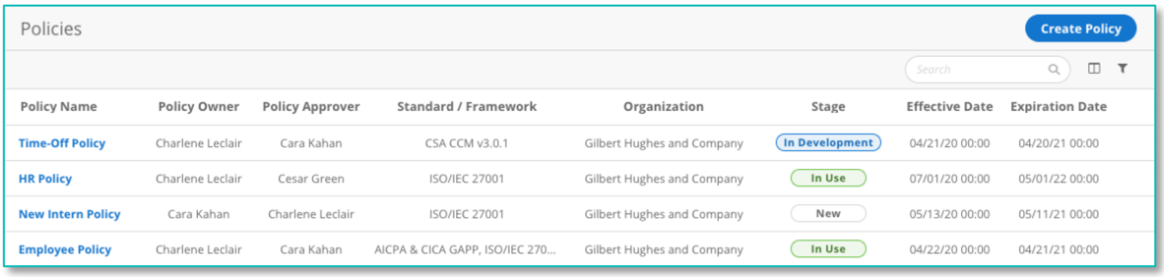
Two questions to ask when determining clarity of policies:

- *Are our policies documented clearly enough for those we expect to follow them?*
- *Are the roles and responsibilities defined well enough to be carried out by those assigned to them?*

Execution in One Trust

1. Creating a new policy

Policies are guided by customizable workflows within the tool (like other content we have explored in this course), but this module also includes a policy builder that is specifically designed for the placement and organization of policies.



Policies

Policy Name	Policy Owner	Policy Approver	Standard / Framework	Organization	Stage	Effective Date	Expiration Date
Time-Off Policy	Charlene Leclair	Cara Kahan	CSA CCM v3.0.1	Gilbert Hughes and Company	In Development	04/21/20 00:00	04/20/21 00:00
HR Policy	Charlene Leclair	Cesar Green	ISO/IEC 27001	Gilbert Hughes and Company	In Use	07/01/20 00:00	05/01/22 00:00
New Intern Policy	Cara Kahan	Charlene Leclair	ISO/IEC 27001	Gilbert Hughes and Company	New	05/13/20 00:00	05/11/21 00:00
Employee Policy	Charlene Leclair	Cara Kahan	AICPA & CICA GAPP, ISO/IEC 270...	Gilbert Hughes and Company	In Use	04/22/20 00:00	04/21/21 00:00

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

Step 2: Click on Enterprise Management

Step 3: Click the Policies Tab on the left side of the screen

Step 4: Click the Blue Add New Button in the centre of the screen

Step 5: for Name, type in System Security Policy

Step 6: For Organization, Select OneTrust

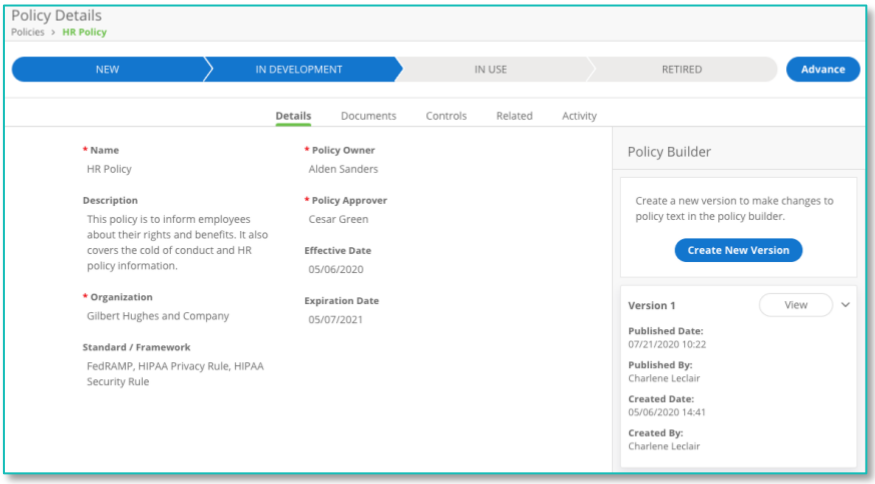
Step 7: Select a Policy Owner and Policy Approver

Step 8: Select an Effective Date

Step 9: Click the Blue Create Button at the bottom right of the screen

2. Building and editing a policy

In this exercise, the Policy Approver places guidelines into the policy builder for the completion of policies by the Policy Owner.



* Name: HR Policy

Description: This policy is to inform employees about their rights and benefits. It also covers the cold of conduct and HR policy information.

* Organization: Gilbert Hughes and Company

Standard / Framework: FedRAMP, HIPAA Privacy Rule, HIPAA Security Rule

* Policy Owner: Alden Sanders

* Policy Approver: Cesar Green

Effective Date: 05/06/2020

Expiration Date: 05/07/2021

Create a new version to make changes to policy text in the policy builder.

Version 1

Published Date: 07/21/2020 10:22

Published By: Charlene Leclair

Created Date: 05/06/2020 14:41

Created By: Charlene Leclair

Step 1: Click the Blue Go to Builder Button on the middle right section of the screen

Step 2: Click the White Add Section Button at the top left of the screen

Step 3: For Section Name, enter Database User Management

Step 4: Select an Icon and Click Done

Step 5: In the free type section below, type in the following phrases:

“Default Policy Statement: Default Policy Procedures: Baseline Recommendations:”

Step 6: Click the White Add Section Button at the top left of the screen

Step 7: For Section Name, enter User Authentication

Step 8: Select an Icon and Click Done

Step 9: In the free type section below, type in the following phrases:

“Default Policy Statement: Default Policy Procedures: Baseline Recommendations:”

Step 10: Click the White Add Section Button at the top left of the screen

Step 11: For Section Name, enter Operating System Security

Step 12: Select an Icon and Click Done

Step 13: In the free type section below, type in the following phrases:

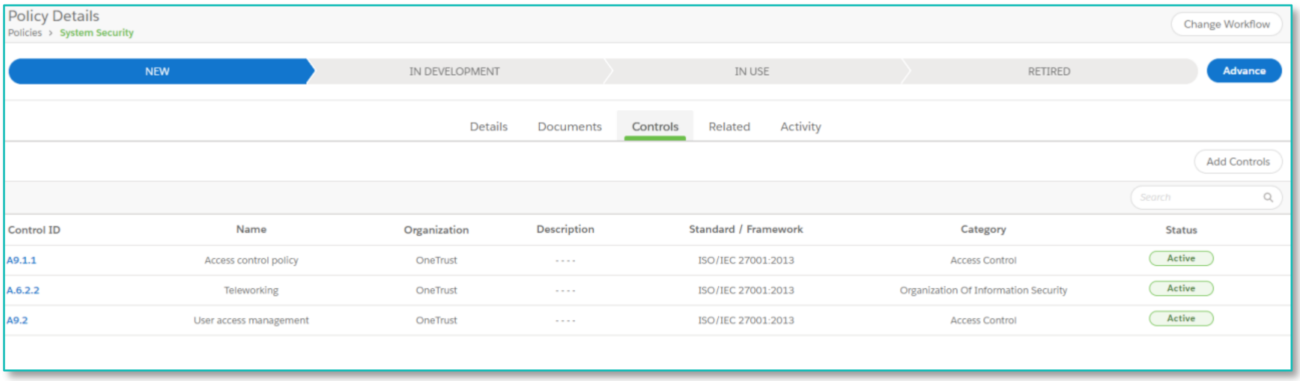
“Default Policy Statement: Default Policy Procedures: Baseline Recommendations:”

Step 14: Click the White Save Button at the top right of the screen

Step 15: Click the Blue Publish Button at the top right of the screen

3. Adding controls to enforce a policy

In this exercise, you can attach controls to assist in making sure your policy is observed, implemented, and reviewed according to either controls specific to your organization OR a standard or framework your policy will need to adhere to.


Policy Details
Policies › System Security

Control ID	Name	Organization	Description	Standard / Framework	Category	Status
A9.1.1	Access control policy	OneTrust	----	ISO/IEC 27001:2013	Access Control	Active
A.6.2.2	Teleworking	OneTrust	----	ISO/IEC 27001:2013	Organization Of Information Security	Active
A9.2	User access management	OneTrust	----	ISO/IEC 27001:2013	Access Control	Active

Step 1: Click on the Policies Tab at the top left of the screen

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 Blue Add Control Button in the Center of the Screen

Step 5: For Standard/Framework select ISO/IEC 27001:2013 on the left side of the screen

Step 6: In the Search Bar at the top right, type in 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.6,

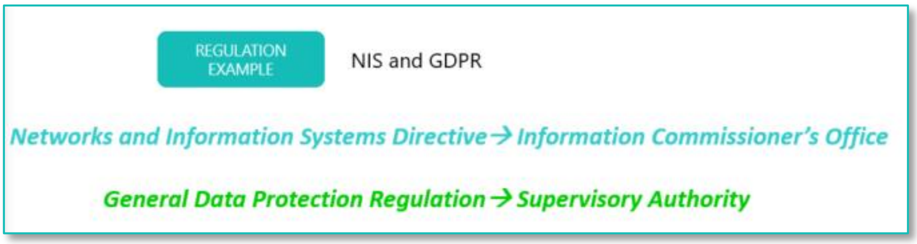
Step 10: Check the box for A.6.2.2 Teleworking

Step 11: Click the Blue Add Button at the Bottom Right of the Menu

Incidents Management

When incidents do occur, it is 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.

Module Overview



REGULATION EXAMPLE NIS and GDPR

Networks and Information Systems 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.

METHOD EXAMPLE Breach Response Plan

A Breach Response Plan provides guideline 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.

Operational Best Practices

Know Associated Assessments

One of the types of questions in the template question builder is the Incident Question Type. Using Assessment questions with this question type will populate details within incidents. Different types of assessments can be used to report on specific details within specific types of incidents.

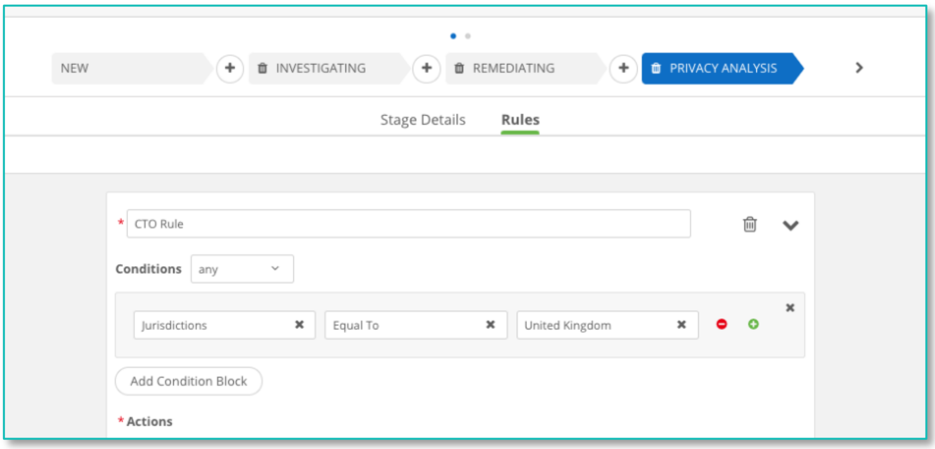
Assign Risks to Specific Owners

Within the incident workflows, directly responsible individuals can be assigned tasks and specific contacts can be notified. These assignments and notifications will allow centralized communication, better tracking of accountability, and improved response time.

Execution in One Trust

1. Creating a workflow to process incidents

In this exercise, a workflow and custom stage with rules within the workflow is created for the intake, evaluation, and processing of specific types of incidents.



* CTO Rule

Conditions any

Jurisdictions | Equal To | United Kingdom

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

Step 2: Click on Incident Response

Step 3: Go to the Setup tab area on the middle left side of the screen

Step 4: Click on the Workflows & Rules Tab on the left side of the screen

Step 5: Click on the Default Workflow

Step 6: Click the White Clone Button at the top Right of the Screen

Step 7: For workflow name, type in Data Breach Workflow

Step 8: Click the Blue Clone Button

<u>Part 2</u>

Step 1: Click into your new workflow

Step 2: At the top middle of the screen, click the plus button in between investigating and remediating

Step 3: For stage name type in Risk analysis

Step 4: Click the blue add button at the bottom right of the menu

Step 5: Click on the Rules tab

Step 6: Click the Blue Add Rule button at the centre of the screen

Step 7: For Rule Name, type in Notify CIO

Step 8: For the Actions Dropdown, select Send Notification

Step 9: For recipients, first type in your email, then click "assign to (your email)" below the field

Step 10: For Subject enter Data Breach Occurrence

Step 11: For Body, enter There has been a data breach, please visit incident register for more details

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

Step 13: Click the Blue Publish Button at the top right of the screen

Step 14: Click the Blue Publish Button in the centre of the screen

Part 3

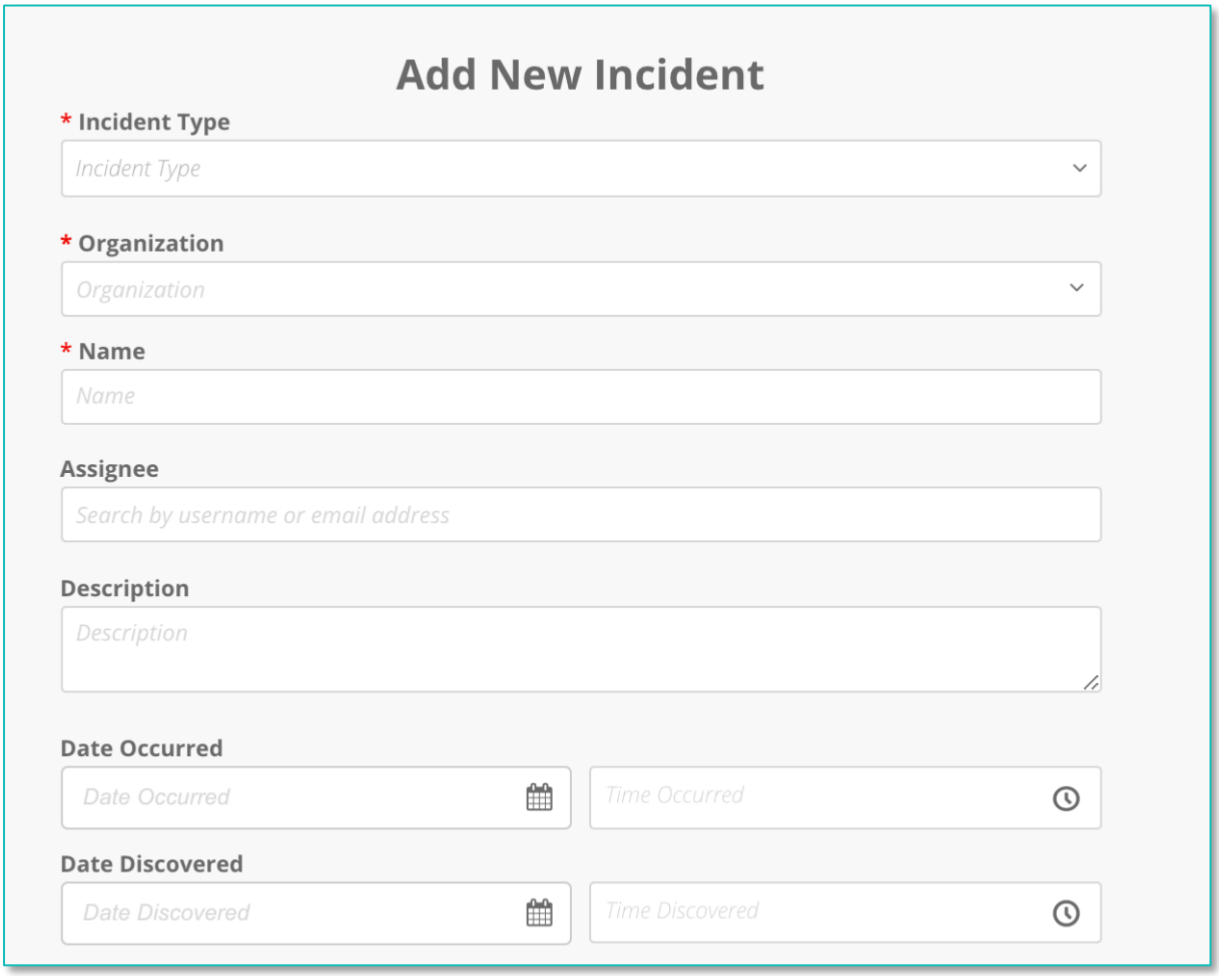
Step 1: Click the … Button to the far right of your new workflow

Step 2: Click set as default

Step 3: Click the Confirm

2. Register an Incident

In the last exercise, a workflow was created for the intack of an incident. This exercise involves entering an incident using the manual interface within the module.



Add New Incident

* Incident Type
Incident Type

* Organization
Organization

* Name
Name

Assignee
Search by username or email address

Description
Description

Date Occurred
Date Occurred
Time Occurred

Date Discovered
Date Discovered
Time Discovered

Step 1: Click the Incident Register Tab at the top left of the screen

Step 2: Click the blue add new button at the top right of the screen

Step 3: For incident type dropdown, select User Account Compromise

Step 4: For Organization, select OneTrust

Step 5: For Name, type in Data Breach via Unauthorized Access

Step 6: For Description, type in a description of your choice

Step 7: Choose a Date for Date Occurred

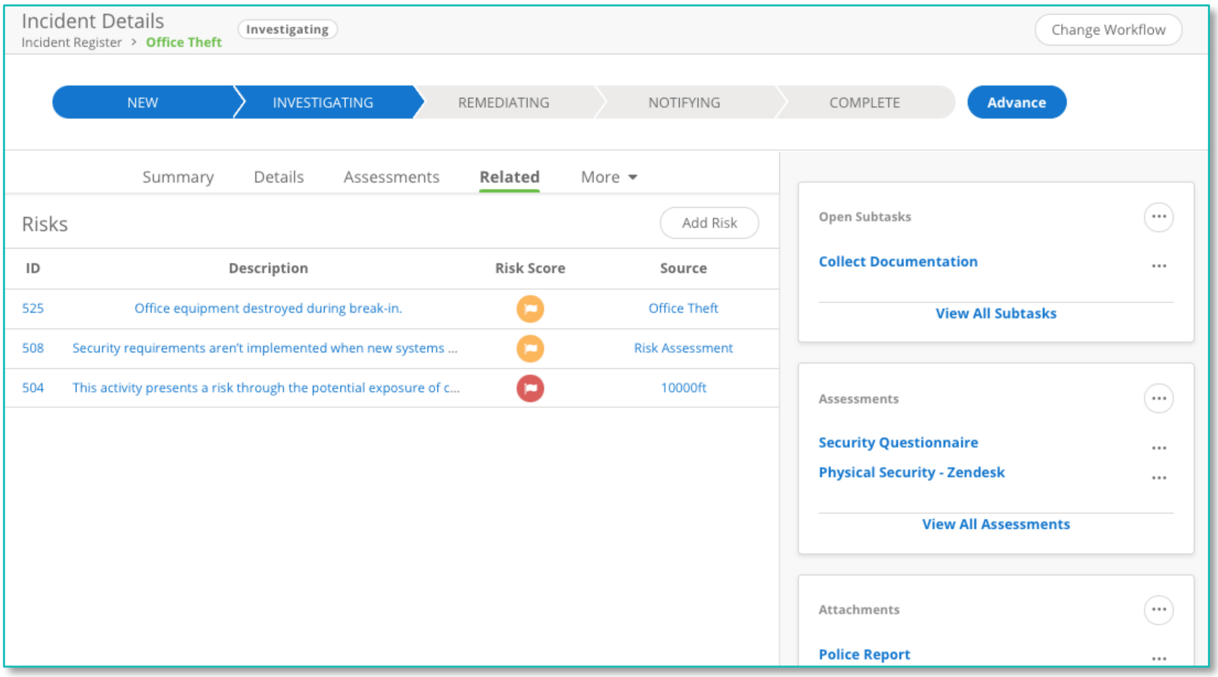
Step 8: Choose a Date for Date Discovered

Step 9: Type in a root cause of your choice

Step 10: Click the White Save Button at the bottom right of the screen

3. Link Incidents with Risks

While processing an incident related risks can be linked in addition to addressing existing subtasks, related assessments, and other items.



Incident Details Investigating
Incident Register > Office Theft

Risks

ID	Description	Risk Score	Source
525	Office equipment destroyed during break-in.	🟧	Office Theft
508	Security requirements aren't implemented when new systems ...	🟧	Risk Assessment
504	This activity presents a risk through the potential exposure of c...	🟥	10000ft

Open Subtasks
Collect Documentation
View All Subtasks

Assessments
Security Questionnaire
Physical Security - Zendesk
View All Assessments

Attachments
Police Report

Step 1: Click the Incident Register Tab at the top left of the screen

Step 2: Click into the incident you created in the previous exercise

Step 3: Click on the Risk Analysis stage at the top middle of the screen

Step 4: Click on the More Tab and Select Related

Step 5: Click the Blue Add Risk Button in the middle of the screen

Step 6: Either select the risk you created earlier by checking the box next to it if you see it, OR you can select a new risk OR create a new risk

Step 7: After choosing a risk, click the Blue Link to incident button

Whistle-blower and Ethics Case Management

The Ethics portal empowers anonymous whistleblowers and other users to submit accounts of alleged ethics violations.

Module Overview

Ethics portals guide a user through case creation and anonymous submission so an internal compliance team can triage, investigate, and respond to cases received by their organization.

The Whistleblower and Ethics Case Management module is currently available by request only. Please contact your account executive to have it set up and enabled for your account environment.

Operational Best Practices

Manage Case Access Permissions

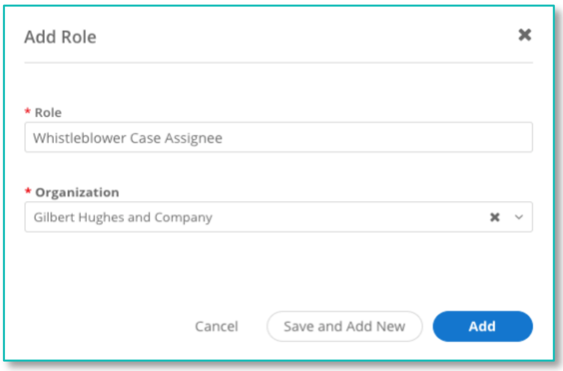
OneTrust grants administrators the ability to add users and assign them role-based access and permissions. A great use for this is the Whistleblower roles, which can allow you to designate specific case assignees and case managers for whisteblower applications utilized with the ethics portal.

The Whistleblower and Ethics Case Management module takes several security precautions in protecting a case submitter's anonymity and privacy. To help comply with this approach, only OneTrust users with explicitly defined roles and permissions will be eligible for case assignment to restrict access to complaints and cases which may be sensitive in nature.

Eligible case admins must be manually assigned during portal configuration or enabled on the case details. This prevents users on your compliance team from mistakenly or accidentally gaining access to a case which might compromise anonymity. The assignee role permission enables a user to be eligible for a case assignment, while the Manager role enables a user to be a fully authorized admin in the Whistleblower and Ethics Case Management Module

Execution in One Trust

1. Configure Roles & Intake Forms



Add Role

* Role: Whistleblower Case Assignee

* Organization: Gilbert Hughes and Company

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

Step 2: Click on Users and Groups

Step 3: Click on a desired User

Step 4: Click on the Roles tab in the upper middle of the screen

Step 5: Click the white add Role Button at the top right of the screen

Step 6: For Organization, select OneTrust

Step 7: For Role, select Whistle-blower Manager

Step 8: Click the blue add button at the bottom right of the menu

Step 9: Click the Users tab on the left middle side of the screen

Step 10: Click another desired user (different than the one you chose previously)

Step 11: Click on the Roles tab in the upper middle of the screen

Step 12: Click the white add Role Button at the top right of the screen

Step 13: For Organization, select OneTrust

Step 14: For Role, select Whistleblower Case Assignee

Part 2

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

Step 2: Click on Whistle-blower & Ethic Case Management

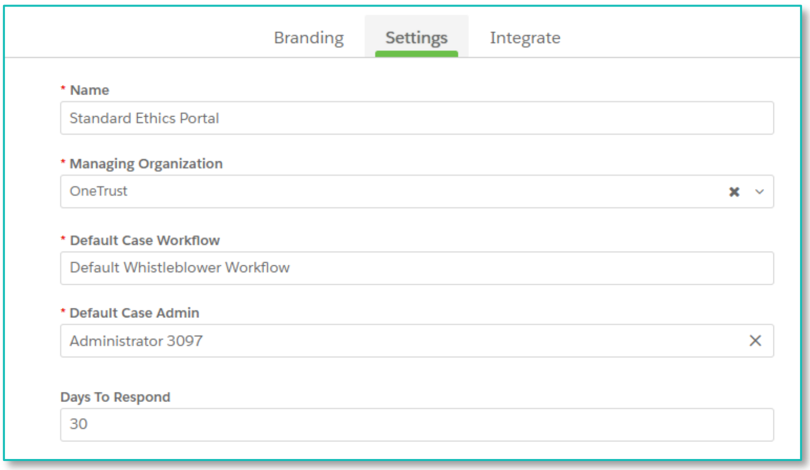
Step 3: Click the Intake Forms tab on the left side of the screen

Step 4: Click the Blue Create button in the middle of the screen

Step 5: For Name, enter Standard Intake Form

Step 6: Click the Blue Create button on the bottom right of the screen

2. Configuring Ethics Portal



* Name
Standard Ethics Portal

* Managing Organization
OneTrust

* Default Case Workflow
Default Whistleblower Workflow

* Default Case Admin
Administrator 3097

Days To Respond
30

Step 1: Click on the Launch Pad Icon

Step 2: Click on Whistle-blower & Ethic Case Management

Step 3: Click on the Ethics Portal tab on the left side of the screen

Step 4: Click the Blue Create Button in the middle of the screen

Step 5: for Name, enter ethics portal

Step 6: For Managing Organization, select OneTrust

Step 7: For Fulfillment Workflow, select Default Whistle-blower Workflow

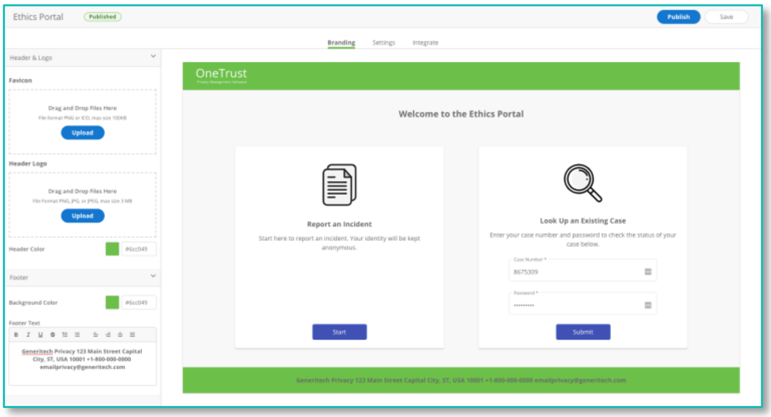
Step 8: For Intake Form, select standard form

Step 9: For Default Approver, select yourself

Step 10: Click the blue create button at the bottom right of the screen

3. Configuring the portal branding

This exercise involves adjusting the look and feel of the ethics portal to appear as a natural inclusion to your website.



Welcome to the Ethics Portal

Report an Incident

Start here to report an incident. Your identity will be kept anonymous.

Look Up an Existing Case

Enter your case number and password to check the status of your case below.

Case Number * 8675309

Password * ••••••••••

Header Color #6cc049

Background Color #6cc049

Footer Text: Generitech Privacy 123 Main Street Capital City, ST, USA 10001 +1-800-000-0000 emailprivacy@generitech.com

Generitech Privacy 123 Main Street Capital City, ST, USA 10001 +1-800-000-0000 emailprivacy@generitech.com

Step 1: Click on the Branding Tab at the middle left of the screen

Step 2: Click the blue upload button for the header logo section

Step 3: Upload an appropriate image from your computer such as your own company's logo

Step 4: Click the Header Colour Block and select a desired colour

Step 5: Click the white save button at the top right of the screen

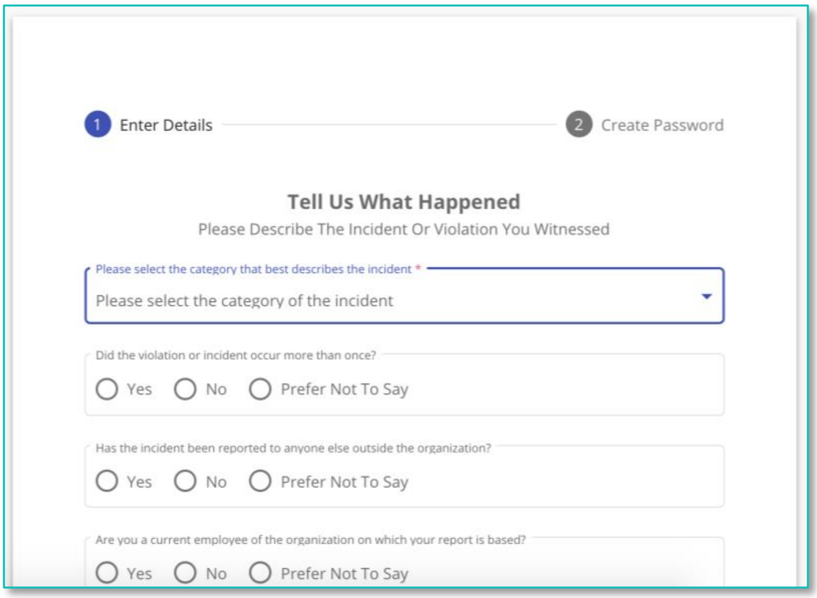
Step 6: Click the blue Publish button at the top right of the screen

Step 7: Click the Blue Publish Button in the middle of the screen

Step 8: Leave the existing pop up box "successfully published" up without closing it

4. Log a case

This exercise involves testing the forms that were previously created to ensure case submission can be entered properly.



Tell Us What Happened

Please Describe The Incident Or Violation You Witnessed

Please select the category that best describes the incident *

Please select the category of the incident

Did the violation or incident occur more than once?

○ Yes ○ No ○ Prefer Not To Say

Has the incident been reported to anyone else outside the organization?

○ Yes ○ No ○ Prefer Not To Say

Are you a current employee of the organization on which your report is based?

○ Yes ○ No ○ Prefer Not To Say

Step 1: Click the white Test Button in the middle of the screen (this will lead you to another browser)

Step 2: Click the start button for Report an Incident

Step 3: Fill out the entire form with your own preferred details (this is an imaginary case)

Step 4: Once all fields are filled, click the next button at the bottom right of the screen

Step 5: Enter your own unique password (follow the guidelines at the bottom of the screen)

Step 6: Click the submit button at the bottom right of the screen

Audit Management

OneTrust Audit Management Module enables the application of a risk-based approach to an organization’s GRC audit efforts to recognize the scope of business practices, their impact and where proposed measures for improvement can be effectively implemented.

Module Overview

The Audit Management Module automates the work streams of audit teams, optimizing resources and productivity. It is an assessment of methods and policies of an organization's management in the administration and the use of resources, tactical and strategic planning, and employee and organizational improvement.

Objective:
- Simplify and organize the workflow and collaboration process of compiling audits.
- Ensuring that board-approved audit directives are implemented

AUDITS WORKPAPERS FINDINGS

Operational Best Practices

Define audit scope

- Decide what risks are being tracked or which Standard or Framework is to be utilized.
- Plan your Work Paper, which is the document that records during the course of an audit the audit evidence obtained during various types of auditing, including financial statements auditing, internal management auditing, information systems auditing, and investigations.
- Assign an auditor. This role should be independent of an organization’s management so that the audit is unbiased.

Test controls

These three aspects of the controls should be tested:

- The implementations of the controls you will be auditing against
- The Design and Effectiveness of the controls

- The record of their activity

Consolidate findings

- After the auditor has completed their work, findings need to be consolidated. Once all evidence is gathered, it should be reviewed in detail to identify any audit findings.
- This review is done based on historical understanding of the process, historical evidence obtained, and auditor professional judgement on the adequacy of the evidence provided.

Apply Recommendations

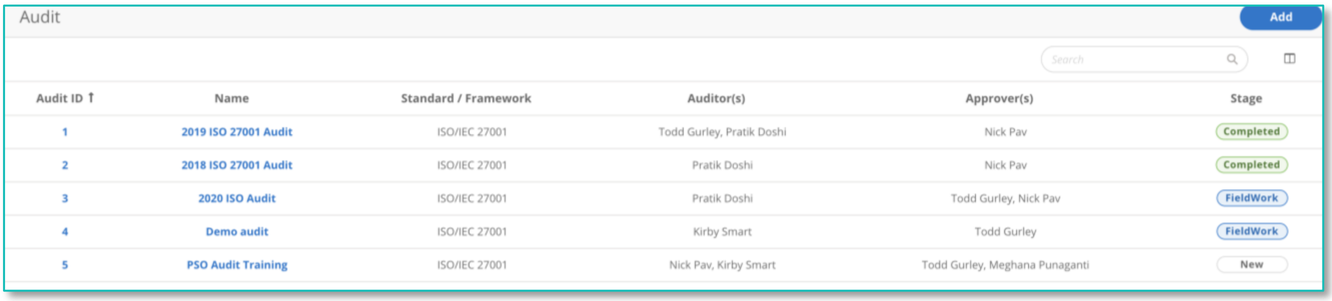
Based on auditor findings, management will need to recommend compensating or complementary controls to address the risks identified in the audit. What is the effect of these controls on the risks identified and do they reduce the residual risk to an acceptable amount? Lastly, what is the frequency of our audits (when will we re-assess the findings)?

Execution in One Trust

1. Add a new Audit

This exercise includes naming the audit, selecting a standard, defining objectives, planned time period, and who will actually perform the audit as well as who will review and ultimately approve the project.

When a standard/framework is selected, controls can be selected from that framework and different auditors can be assigned to each control.



Audit ID ↑	Name	Standard / Framework	Auditor(s)	Approver(s)	Stage
1	2019 ISO 27001 Audit	ISO/IEC 27001	Todd Gurley, Pratik Doshi	Nick Pav	Completed
2	2018 ISO 27001 Audit	ISO/IEC 27001	Pratik Doshi	Nick Pav	Completed
3	2020 ISO Audit	ISO/IEC 27001	Pratik Doshi	Todd Gurley, Nick Pav	FieldWork
4	Demo audit	ISO/IEC 27001	Kirby Smart	Todd Gurley	FieldWork
5	PSO Audit Training	ISO/IEC 27001	Nick Pav, Kirby Smart	Todd Gurley, Meghana Punaganti	New

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

Step 2: Click on Audit Management

Step 3: Click on the Audits Tab on the upper left side of the screen

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

Step 5: For Audit Name, type in Privacy Audit 2020

Step 6: For Standard/Framework Dropdown, select NIST SP 800 rev4

Step 7: For Organization, select OneTrust

Step 8: For Auditor and recipient, select your admin profile name "Admin…"

Step 9: Click the Blue Next Button at the bottom right of the screen

Step 10: For Scope, check the box next to AC-11 Session Lock

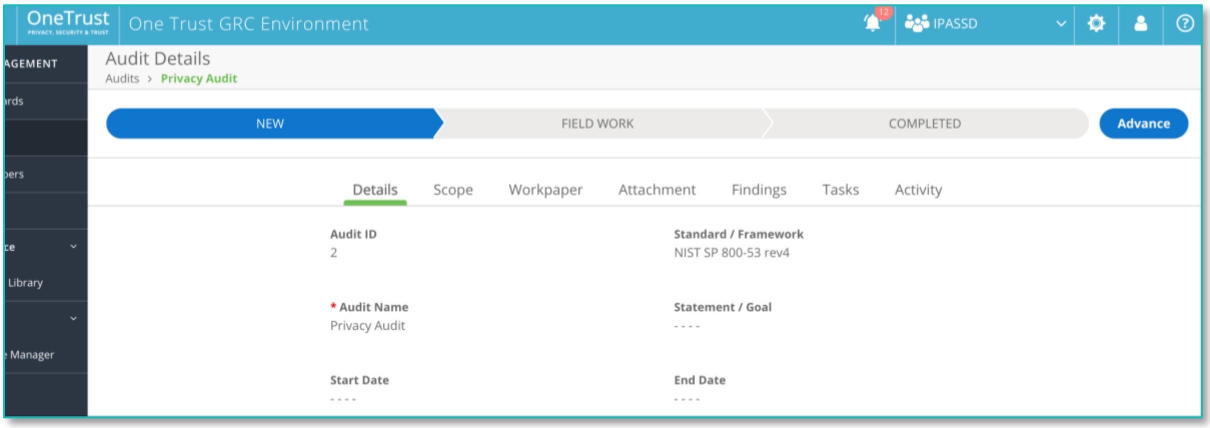
Step 11: Click the Blue Next Button at the bottom right of the screen

Step 12: For Assign Auditors, Click the Select All Checkbox and then assign your admin profile name, "admin…."

Step 13: Click the Blue Start Button at the bottom right of the screen

Step 14: Click the Blue Create Button in the center of the screen

2. Complete a workpaper



Audit Details

Audits › Privacy Audit

Audit ID
2

Standard / Framework
NIST SP 800-53 rev4

* Audit Name
Privacy Audit

Statement / Goal

Start Date

End Date

Step 1: In the new stage of your audit details page, click the Workpaper tab in the top middle of the screen

Step 2: Click on the ID Number for AC-11 Session Lock

Step 3: Click on the Findings Tab in the top middle of the screen

Step 4: Click the White Log Finding Button in the middle of the screen

Step 5: For the Please Identify the type of finding Dropdown, select Opportunity for Improvement

Step 6: For Finding, type in Laptops are missing autolocking profile feature

Step 7: Click the Blue Save Button at the bottom right of the menu

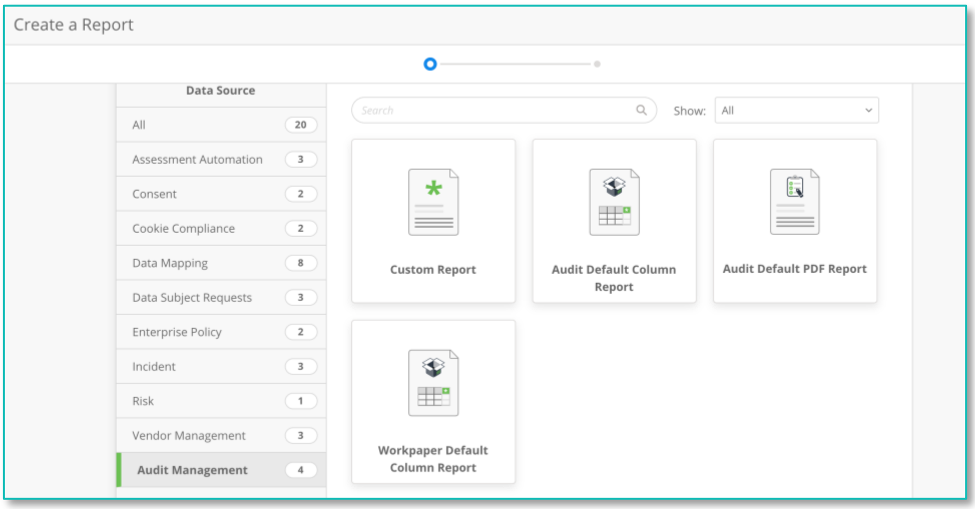
Step 8: Click on the finding ID number for the finding you just created

Step 9: At the bottom of the screen, go to action plan and click the edit button to the right of action detail (you may have to hover the mouse to the right of action plan)

Step 10: For Action Plan, type in the text: Implementing Autolocking profile features

Step 11: Click the blue Save button at the bottom right of the screen

3. Create an Audit Report



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

Step 2: Click on Reports on the right side of the menu

Step 3: Click the Blue Create New Button at the top right of the screen

Step 4: For Data Source on the left side of the menu select Audit Management

Step 5: Click on the box for Audit Default Column Report

Step 6: Click the Blue Next Button at the bottom right of the screen

Step 7: For Report Name, type in Audit Report 2020

Step 8: Click the Blue Create Button at the bottom right of the screen

Step 9: Make any desired changes to columns and click the white save button at the top of the screen IF changes are made

Step 10: Click the Blue Export Button at the top right of the screen

Step 11: Click the Close Button in the Middle of the Screen

Step 12: Click the White Bell Logo at the top right of the screen

Step 13: If you wish, click on the report name to download

Exam Review

OneTrust GRC Professional Certification Exam

Format: non – proctored, online

Duration: 90 minutes

Questions: 35 (all multiple choice)

Passing Score: 80%

Certification Validity: 1 year

Exam Breakdown

10% Module Overview

20% Best Practices

70% Execution in OneTrust

Glossary

A

Assessment – A list of questions assigned to a respondent within the OneTrust tool that requires 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 guideline 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 which 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 & behaviour 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.