Configuration Manual

MSc Research Project- Industry Internship
MSc Cyber Security

Rishabh Sachdeva
Student ID: X21213909

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rishabh Sachdeva		
Student ID:	X21213909		
Programme:	MSc in Cybersecurity	**Year:**	2022/23
Module:	MSc Research Project - Industry Internship		
Lecturer:	Prof. Vikas Sahni		
Submission Due Date:	04/09/2023		
Project Title:	Developing a Pre-Readiness Compliance Assessment Framework for Financial Institutions under the EU's Digital Operational Resilience Act (DORA) – Configuration Manual		
Word Count:	2648	**Page Count:**	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rishabh Sachdeva

Date: 02/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Rishabh Sachdeva
Student ID: X21213909

1 Introduction

This Configuration Manual is intended to serve as an integral artifact of the research project focused on the DORA Pre-Readiness Compliance Assessment Framework. Created to guide users and thesis assessor through the complexities of assessing compliance levels in relation to the European Union's Digital Operational Resilience Act (DORA), the manual aims to offer comprehensive instructions. Guidelines for software are provided, along with step-by-step procedures for navigating within the Excel template, utilizing the web based OneTrust portal for compliance assessment, and leveraging Power BI for analytics.

The manual has been structured to assist a range of users, from cybersecurity professionals , academic researchers, compliance officers to internal team members of financial institutions. By adhering to the instructions contained herein, effective compliance assessments can be performed, insightful reports can be generated, and assessments can be shared with clients.

It is assumed that a basic understanding of compliance assessment terminologies and general computer literacy are possessed by the users.

2 Software Requirements

In the context of this research project, specific software tools have been identified as essential for the effective implementation and utilization of the DORA Compliance Assessment Framework. The following software requirements have been outlined:

2.1 Microsoft Excel

- **Purpose**: For the manipulation and analysis of compliance data, as well as for the initial stages of template creation.
- **Version**: Microsoft Excel 2019 or later is recommended for compatibility.
- **Download**: Can be obtained as part of the Microsoft Office Suite from the official Microsoft website.

2.2 OneTrust Portal

- **Purpose**: For advanced compliance assessment template creation, report generation, and client sharing.
- **Version**: Latest version accessible via web browser.
- **Access**: The portal can be accessed through the following link: OneTrust Portal. Please note the Portal is accessible only to designated Waystone Employees with access.

2.3 Power BI

- **Purpose**: For analytics and dashboard creation, enabling real-time insights into compliance levels.
- **Version**: Power BI Desktop for report creation; Power BI Service for sharing and collaboration.
- **Download**: Available for download from the official Microsoft Power BI website.

3 Excel Workbook

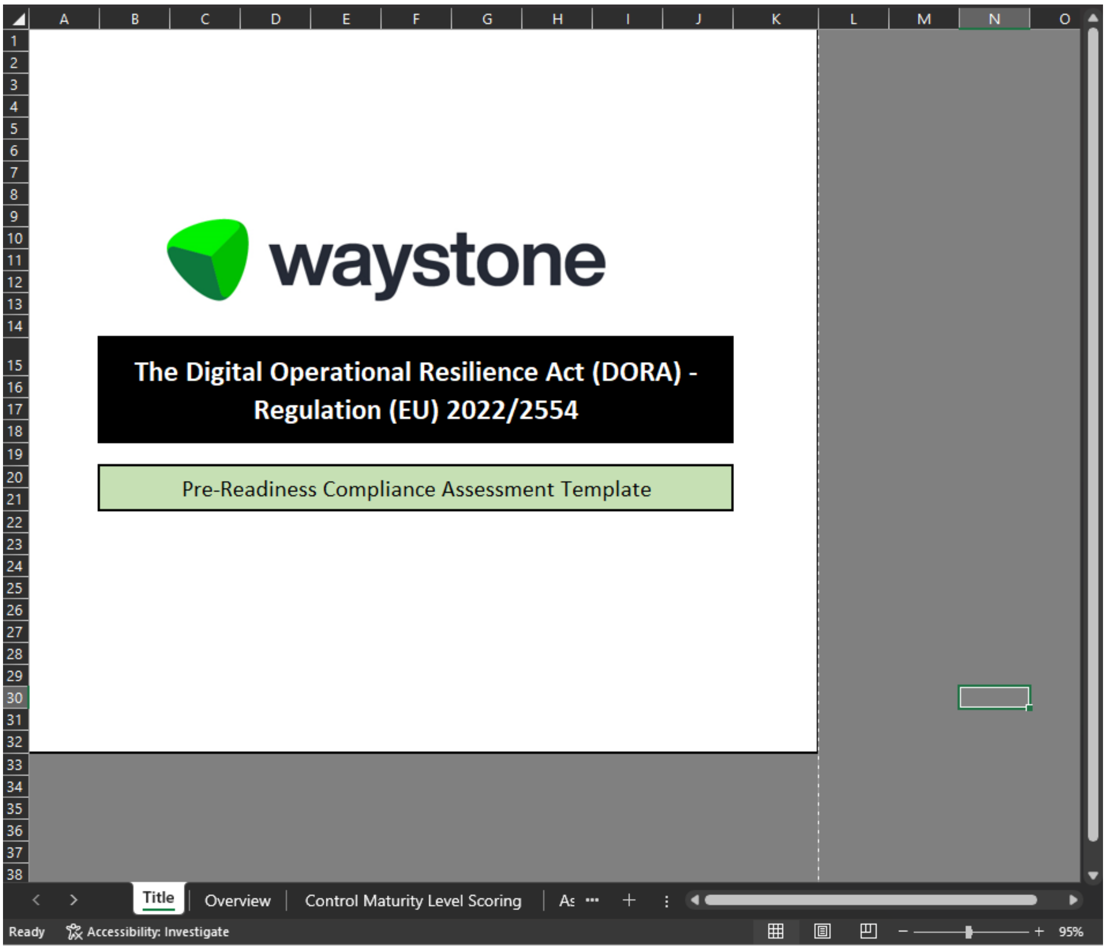
3.1 Configured Structure of the Workbook

The Excel Workbook titled ‘WCS_DORA-(EU) 2022_2554_Compliance Assessment Template_v1.0’ is carefully structured to facilitate a seamless compliance assessment process. It consists of multiple tabs, each serving a unique purpose:

- **Title Sheet**: This is the introductory tab that presents the title and a brief context of the workbook.
- **Overview Sheet**: This comprehensive tab includes the Description, Instructions, Scope, and Subject Matter of the DORA Act, serving as a one-stop guide for users.
- **Assessment Sheet**: This is the core tab where the actual assessment takes place, featuring various columns to capture compliance data.
- **Control Maturity Level Scoring Methodology**: This tab elucidates the scoring system used in the assessment.
- **Visualization Sheet**: This is a normalized data sheet designed for importation into Power BI for further analytics.

3.1.1 Title Sheet

The Title Sheet serves as the introductory page of the workbook, providing the title and setting the context for the assessment.



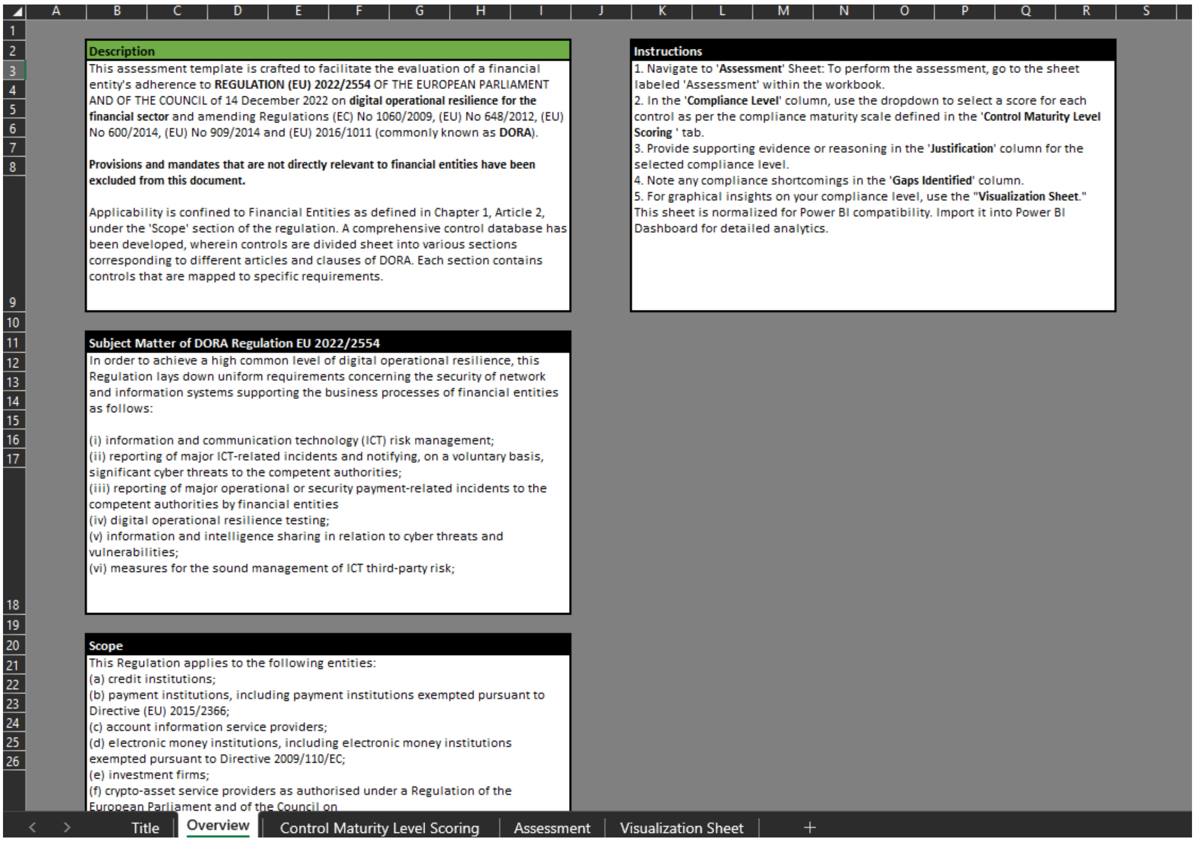
The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554

Pre-Readiness Compliance Assessment Template

Figure 1 Title Sheet

3.1.2 Overview Sheet

The Overview Sheet is a multi-faceted tab designed to provide users with all the essential information they need to conduct the assessment. It is divided into four main sections:



Description

This assessment template is crafted to facilitate the evaluation of a financial entity's adherence to **REGULATION (EU) 2022/2554** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on **digital operational resilience for the financial sector** and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (commonly known as **DORA**).

Provisions and mandates that are not directly relevant to financial entities have been excluded from this document.

Applicability is confined to Financial Entities as defined in Chapter 1, Article 2, under the 'Scope' section of the regulation. A comprehensive control database has been developed, wherein controls are divided sheet into various sections corresponding to different articles and clauses of DORA. Each section contains controls that are mapped to specific requirements.

Instructions

1. Navigate to '**Assessment**' Sheet: To perform the assessment, go to the sheet labeled 'Assessment' within the workbook.
2. In the '**Compliance Level**' column, use the dropdown to select a score for each control as per the compliance maturity scale defined in the '**Control Maturity Level Scoring** ' tab.
3. Provide supporting evidence or reasoning in the '**Justification**' column for the selected compliance level.
4. Note any compliance shortcomings in the '**Gaps Identified**' column.
5. For graphical insights on your compliance level, use the "**Visualization Sheet**." This sheet is normalized for Power BI compatibility. Import it into Power BI Dashboard for detailed analytics.

Subject Matter of DORA Regulation EU 2022/2554

In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(i) information and communication technology (ICT) risk management;
(ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
(iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities
(iv) digital operational resilience testing;
(v) information and intelligence sharing in relation to cyber threats and vulnerabilities;
(vi) measures for the sound management of ICT third-party risk;

Scope

This Regulation applies to the following entities:
(a) credit institutions;
(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
(c) account information service providers;
(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;
(e) investment firms;
(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on

Figure 2 Overview Sheet

- **Description**: This section offers a detailed overview of the assessment template, helping users understand what the workbook aims to achieve.

- **Instructions**: A concise guide on how to perform the assessment is provided here. It walks users through the scoring process, justification, and gap identification, among other things.

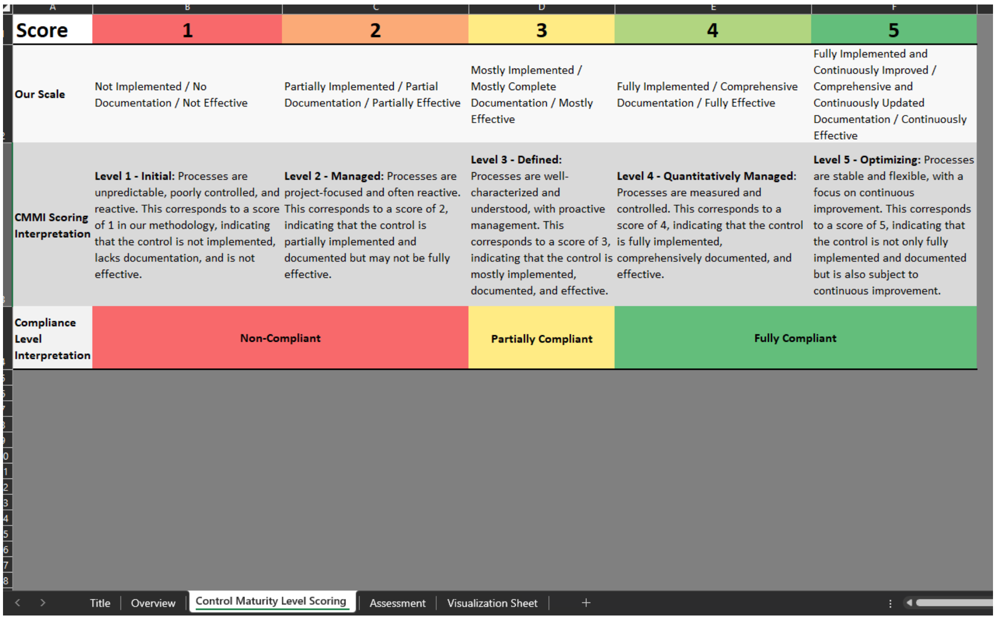
- **Scope**: This section outlines the scope of the DORA regulation as defined in Chapter 1, General Provisions, Article 2. It ensures that users are aware that the assessment is specifically tailored for financial entities as per the DORA Act.

- **Subject Matter**: This part summarizes the subject matter of the DORA Act as outlined in Chapter 1, Article 1. It gives users a comprehensive understanding of the DORA Act's objectives and requirements.

By consulting the Overview Sheet, users are equipped with all the necessary information to navigate the DORA Compliance Assessment Excel Workbook effectively.

3.1.3 Control Maturity Level Scoring Sheet

The Control Maturity Level Scoring Sheet serves as the backbone for the assessment process. It outlines the scoring methodology that should be used when evaluating each control in the Assessment Sheet. The Control Maturity Level Scoring Methodology is a critical component of the Control Maturity Level Scoring Sheet. It provides a standardized approach to evaluating the implementation and effectiveness of controls, aligning with the Capability Maturity Model Integration (CMMI) framework for added context.

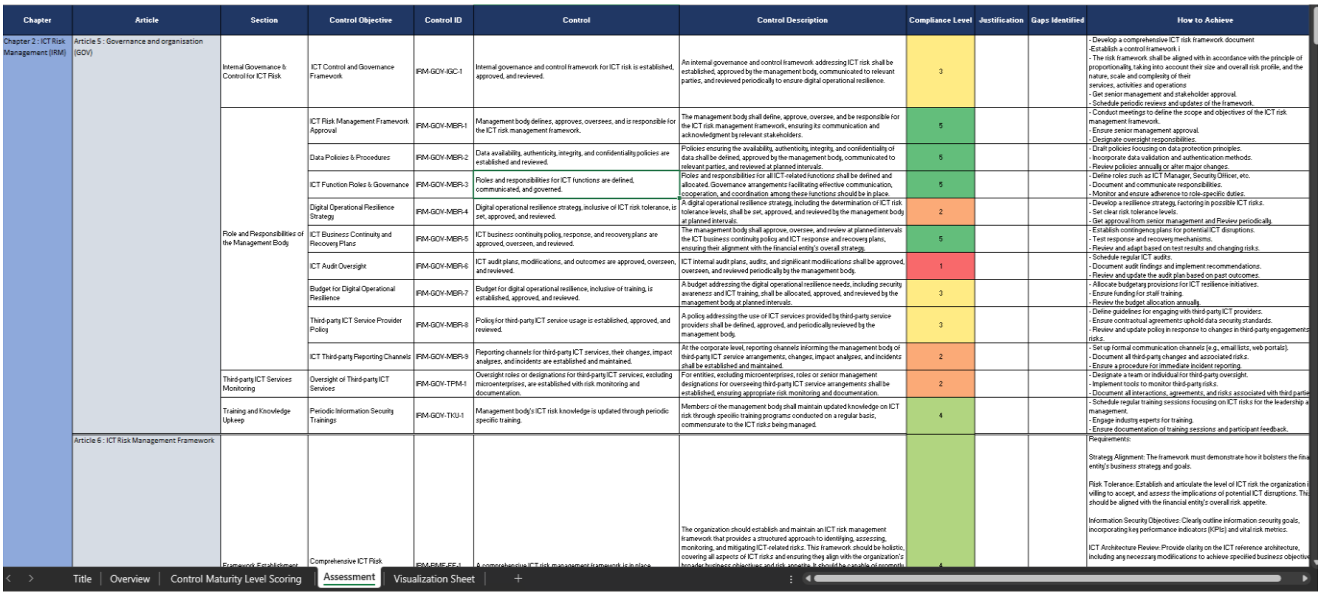


Score	1	2	3	4	5
Our Scale	Not Implemented / No Documentation / Not Effective	Partially Implemented / Partial Documentation / Partially Effective	Mostly Implemented / Mostly Complete Documentation / Mostly Effective	Fully Implemented / Comprehensive Documentation / Fully Effective	Fully Implemented and Continuously Improved / Comprehensive and Continuously Updated Documentation / Continuously Effective
CMMI Scoring Interpretation	**Level 1 - Initial:** Processes are unpredictable, poorly controlled, and reactive. This corresponds to a score of 1 in our methodology, indicating that the control is not implemented, lacks documentation, and is not effective.	**Level 2 - Managed:** Processes are project-focused and often reactive. This corresponds to a score of 2, indicating that the control is partially implemented and documented but may not be fully effective.	**Level 3 - Defined:** Processes are well-characterized and understood, with proactive management. This corresponds to a score of 3, indicating that the control is mostly implemented, documented, and effective.	**Level 4 - Quantitatively Managed:** Processes are measured and controlled. This corresponds to a score of 4, indicating that the control is fully implemented, comprehensively documented, and effective.	**Level 5 - Optimizing:** Processes are stable and flexible, with a focus on continuous improvement. This corresponds to a score of 5, indicating that the control is not only fully implemented and documented but is also subject to continuous improvement.
Compliance Level Interpretation	Non-Compliant		Partially Compliant	Fully Compliant	

Figure 3 Control Maturity Level Scoring Sheet

3.1.4 Assessment Sheet

The Assessment Sheet is where the actual compliance assessment takes place. It is structured to capture a wide range of data, including control objectives, control IDs, compliance levels, justifications, and identified gaps.



Chapter	Article	Section	Control Objective	Control ID	Control	Control Description	Compliance Level	Justification	Gaps Identified	How to Achieve
Chapter 2 : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Internal Governance & Control for ICT Risk	ICT Control and Governance Framework	IRM-GOV-IGC-1	Internal governance and control framework for ICT risk is established, approved, and reviewed.	An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.	3			- Develop a comprehensive ICT risk framework document -Establish a control framework i - The risk framework shall be aligned with in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations - Get senior management and stakeholder approval. - Schedule periodic reviews and updates of the framework.
		Role and Responsibilities of the Management Body	ICT Risk Management Framework Approval	IRM-GOV-MBR-1	Management body defines, approves, oversees, and is responsible for the ICT risk management framework.	The management body shall define, approve, oversee, and be responsible for the ICT risk management framework, ensuring its communication and acknowledgment by relevant stakeholders.	5			- Conduct meetings to define the scope and objectives of the ICT risk management framework. - Ensure senior management approval. - Designate oversight responsibilities.
			Data Policies & Procedures	IRM-GOV-MBR-2	Data availability, authenticity, integrity, and confidentiality policies are established and reviewed.	Policies ensuring the availability, authenticity, integrity, and confidentiality of data shall be defined, approved by the management body, communicated to relevant parties, and reviewed at planned intervals.	5			- Draft policies focusing on data protection principles. - Incorporate data validation and authentication methods. - Review policies annually or after major changes.
			ICT Function Roles & Governance	IRM-GOV-MBR-3	Roles and responsibilities for ICT functions are defined, communicated, and governed.	Roles and responsibilities for all ICT-related functions shall be defined and allocated. Governance arrangements facilitating effective communication, cooperation, and coordination among these functions should be in place.	5			- Define roles such as ICT Manager, Security Officer, etc. - Document and communicate responsibilities. - Monitor and ensure adherence to role-specific duties.
			Digital Operational Resilience Strategy	IRM-GOV-MBR-4	Digital operational resilience strategy, inclusive of ICT risk tolerance, is set, approved, and reviewed.	A digital operational resilience strategy, including the determination of ICT risk tolerance levels, shall be set, approved, and reviewed by the management body at planned intervals.	2			- Develop a resilience strategy, factoring in possible ICT risks. - Set clear risk tolerance levels. - Get approval from senior management and Review periodically.
			ICT Business Continuity and Recovery Plans	IRM-GOV-MBR-5	ICT business continuity policy, response, and recovery plans are approved, overseen, and reviewed.	The management body shall approve, oversee, and review at planned intervals the ICT business continuity policy and ICT response and recovery plans, ensuring their alignment with the financial entity's overall strategy.	5			- Establish contingency plans for potential ICT disruptions. - Test response and recovery mechanisms. - Review and adapt based on test results and changing risks.
			ICT Audit Oversight	IRM-GOV-MBR-6	ICT audit plans, modifications, and outcomes are approved, overseen, and reviewed.	ICT internal audit plans, audits, and significant modifications shall be approved, overseen, and reviewed periodically by the management body.	1			- Schedule regular ICT audits. - Document audit findings and implement recommendations. - Review and update the audit plan based on past outcomes.
			Budget for Digital Operational Resilience	IRM-GOV-MBR-7	Budget for digital operational resilience, inclusive of training, is established, approved, and reviewed.	A budget addressing the digital operational resilience needs, including security awareness and ICT training, shall be allocated, approved, and reviewed by the management body at planned intervals.	3			- Allocate budgetary provisions for ICT resilience initiatives. - Ensure funding for staff training. - Review the budget allocation annually.
			Third-party ICT Service Provider Policy	IRM-GOV-MBR-8	Policy for third-party ICT service usage is established, approved, and reviewed.	A policy addressing the use of ICT services provided by third-party service providers shall be defined, approved, and periodically reviewed by the management body.	3			- Define guidelines for engaging with third-party ICT providers. - Ensure contractual agreements uphold data security standards. - Review and update policy in response to changes in third-party engagements risks.
			ICT Third-party Reporting Channels	IRM-GOV-MBR-9	Reporting channels for third-party ICT services, their changes, impact analyses, and incidents are established and maintained.	At the corporate level, reporting channels informing the management body of third-party ICT service arrangements, changes, impact analyses, and incidents shall be established and maintained.	2			- Set up formal communication channels (e.g., email lists, web portals). - Document all third-party changes and associated risks. - Ensure a procedure for immediate incident reporting.
		Third-party ICT Services Monitoring	Oversight of Third-party ICT Services	IRM-GOV-TPM-1	Oversight roles or designations for third-party ICT services, excluding microenterprises, are established with risk monitoring and documentation.	For entities, excluding microenterprises, roles or senior management designations for overseeing third-party ICT service arrangements shall be established, ensuring appropriate risk monitoring and documentation.	2			- Designate a team or individual for third-party oversight. - Implement tools to monitor third-party risks. - Document all interactions, agreements, and risks associated with third partie
		Training and Knowledge Upkeep	Periodic Information Security Trainings	IRM-GOV-TKU-1	Management body's ICT risk knowledge is updated through periodic specific training.	Members of the management body shall maintain updated knowledge on ICT risk through specific training programs conducted on a regular basis, commensurate to the ICT risks being managed.	4			- Schedule regular training sessions focusing on ICT risks for the leadership a management. - Engage industry experts for training. - Ensure documentation of training sessions and participant feedback.
	Article 6 : ICT Risk Management Framework	Framework Establishment	Comprehensive ICT Risk	IRM-RMF-FE-1	A comprehensive ICT risk management framework is in place.	The organization should establish and maintain an ICT risk management framework that provides a structured approach to identifying, assessing, monitoring, and mitigating ICT-related risks. This framework should be holistic, covering all aspects of ICT risks and ensuring they align with the organization's broader business objectives and risk appetite. It should be capable of promptly	4			Requirements: Strategy Alignment: The framework must demonstrate how it bolsters the fina entity's business strategy and goals. Risk Tolerance: Establish and articulate the level of ICT risk the organization i willing to accept, and assess the implications of potential ICT disruptions. Thi should be aligned with the financial entity's overall risk appetite. Information Security Objectives: Clearly outline information security goals, incorporating key performance indicators (KPIs) and vital risk metrics. ICT Architecture Review: Provide clarity on the ICT reference architecture, including any necessary modifications to achieve specified business objective

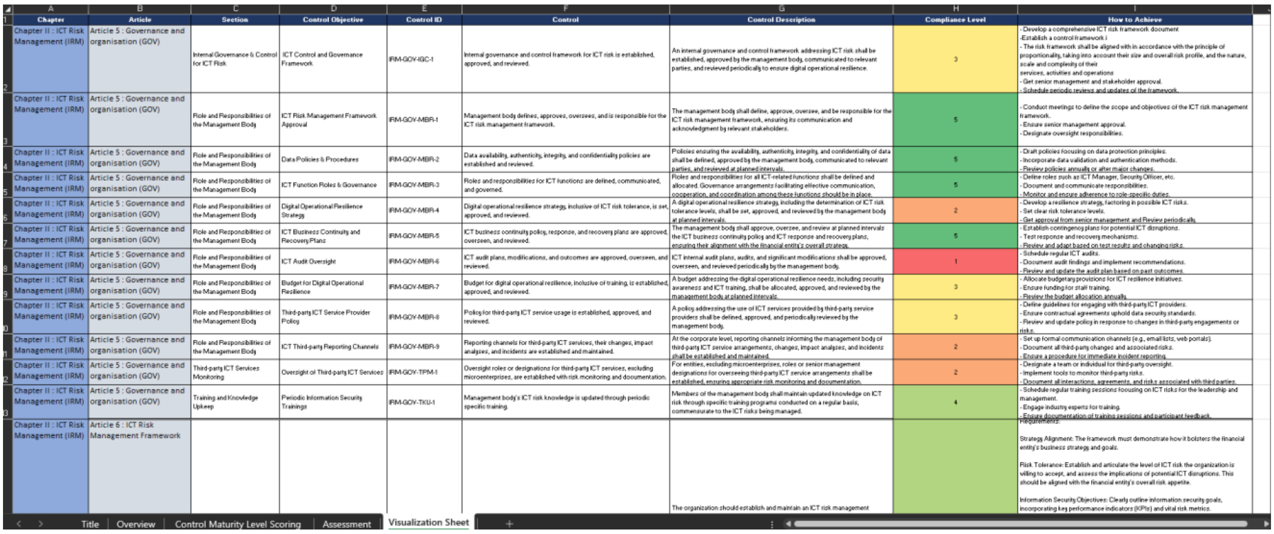
Figure 4 Assessment Sheet

Features

- **Columns**: The sheet features multiple columns such as Chapter, Article, Section, Control Objective, Control ID, Control, Control Description, Compliance Level, Justification, and Gaps Identified. Each column serves a specific purpose in the assessment process.
- **Drop-Down Menus**: The 'Compliance Level' column includes a drop-down menu that allows users to select scores based on the Control Maturity Level Scoring Sheet.

3.1.5 Visualization Sheet

The Visualization Sheet is designed to work in tandem with Power BI to provide insightful analytics based on the assessment data.



Chapter	Article	Section	Control Objective	Control ID	Control	Control Description	Compliance Level	How to Achieve
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Internal Governance & Control for ICT Risk	ICT Control and Governance Framework	IRM-GOV-IGC-1	Internal governance and control framework for ICT risk is established, approved, and reviewed.	An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.	3	- Develop a comprehensive ICT risk framework document -Establish a control framework i - The risk framework shall be aligned with in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations - Get senior management and stakeholder approval. - Schedule periodic reviews and updates of the framework.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	ICT Risk Management Framework Approval	IRM-GOV-MBR-1	Management body defines, approves, oversees, and is responsible for the ICT risk management framework.	The management body shall define, approve, oversee, and be responsible for the ICT risk management framework, ensuring its communication and acknowledgment by relevant stakeholders.	5	- Conduct meetings to define the scope and objectives of the ICT risk management framework. - Ensure senior management approval. - Designate oversight responsibilities.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	Data Policies & Procedures	IRM-GOV-MBR-2	Data availability, authenticity, integrity, and confidentiality policies are established and reviewed.	Policies ensuring the availability, authenticity, integrity, and confidentiality of data shall be defined, approved by the management body, communicated to relevant parties, and reviewed at planned intervals.	5	- Draft policies focusing on data protection principles. - Incorporate data validation and authentication methods. - Review policies annually or after major changes.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	ICT Function Roles & Governance	IRM-GOV-MBR-3	Roles and responsibilities for ICT functions are defined, communicated, and governed.	Roles and responsibilities for all ICT-related functions shall be defined and allocated. Governance arrangements facilitating effective communication, cooperation, and coordination among these functions should be in place.	5	- Define roles such as ICT Manager, Security Officer, etc. - Document and communicate responsibilities. - Monitor and ensure adherence to role-specific duties.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	Digital Operational Resilience Strategy	IRM-GOV-MBR-4	Digital operational resilience strategy, inclusive of ICT risk tolerance, is set, approved, and reviewed.	A digital operational resilience strategy, including the determination of ICT risk tolerance levels, shall be set, approved, and reviewed by the management body at planned intervals.	2	- Develop a resilience strategy, factoring in possible ICT risks. - Set clear risk tolerance levels. - Get approval from senior management and Review periodically.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	ICT Business Continuity and Recovery Plans	IRM-GOV-MBR-5	ICT business continuity policy, response, and recovery plans are approved, overseen, and reviewed.	The management body shall approve, oversee, and review at planned intervals the ICT business continuity policy and ICT response and recovery plans, ensuring their alignment with the financial entity's overall strategy.	5	- Establish contingency plans for potential ICT disruptions. - Test response and recovery mechanisms. - Review and adapt based on test results and changing risks.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	ICT Audit Oversight	IRM-GOV-MBR-6	ICT audit plans, modifications, and outcomes are approved, overseen, and reviewed.	ICT internal audit plans, audits, and significant modifications shall be approved, overseen, and reviewed periodically by the management body.	1	- Schedule regular ICT audits. - Document audit findings and implement recommendations. - Review and update the audit plan based on past outcomes.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	Budget for Digital Operational Resilience	IRM-GOV-MBR-7	Budget for digital operational resilience, inclusive of training, is established, approved, and reviewed.	A budget addressing the digital operational resilience needs, including security awareness and ICT training, shall be allocated, approved, and reviewed by the management body at planned intervals.	3	- Allocate budgetary provisions for ICT resilience initiatives. - Ensure funding for staff training. - Review the budget allocation annually.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	Third-party ICT Service Provider Policy	IRM-GOV-MBR-8	Policy for third-party ICT service usage is established, approved, and reviewed.	A policy addressing the use of ICT services provided by third-party service providers shall be defined, approved, and periodically reviewed by the management body.	3	- Define guidelines for engaging with third-party ICT providers. - Ensure contractual agreements uphold data security standards. - Review and update policy in response to changes in third-party engagements or risks.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Role and Responsibilities of the Management Body	ICT Third-party Reporting Channels	IRM-GOV-MBR-9	Reporting channels for third-party ICT services, their changes, impact analyses, and incidents are established and maintained.	At the corporate level, reporting channels informing the management body of third-party ICT service arrangements, changes, impact analyses, and incidents shall be established and maintained.	2	- Set up formal communication channels (e.g., email lists, web portals). - Document all third-party changes and associated risks. - Ensure a procedure for immediate incident reporting.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Third-party ICT Services Monitoring	Oversight of Third-party ICT Services	IRM-GOV-TPM-1	Oversight roles or designations for third-party ICT services, excluding microenterprises, are established with risk monitoring and documentation.	For entities, excluding microenterprises, roles or senior management designations for overseeing third-party ICT service arrangements shall be established, ensuring appropriate risk monitoring and documentation.	2	- Designate a team or individual for third-party oversight. - Implement tools to monitor third-party risks. - Document all interactions, agreements, and risks associated with third parties.
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	Training and Knowledge Upkeep	Periodic Information Security Trainings	IRM-GOV-TKU-1	Management body's ICT risk knowledge is updated through periodic specific training.	Members of the management body shall maintain updated knowledge on ICT risk through specific training programs conducted on a regular basis, commensurate to the ICT risks being managed.	4	- Schedule regular training sessions focusing on ICT risks for the leadership and management. - Engage industry experts for training. - Ensure documentation of training sessions and participant feedback.
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework					The organization should establish and maintain an ICT risk management		Requirements: Strategy Alignment: The framework must demonstrate how it bolsters the financial entity's business strategy and goals. Risk Tolerance: Establish and articulate the level of ICT risk the organization is willing to accept, and assess the implications of potential ICT disruptions. This should be aligned with the financial entity's overall risk appetite. Information Security Objectives: Clearly outline information security goals, incorporating key performance indicators (KPIs) and vital risk metrics.

Figure 5 Visualization Sheet

- **Features**

- **Normalized Data**: This sheet contains normalized data that is structured for easy importation into Power BI.

- **Formula-Linked**: The sheet is formula-linked to the Assessment Sheet. Any changes made in the Assessment Sheet are automatically reflected in the Visualization Sheet, ensuring real-time updates.
- **Analytics**: Once imported into Power BI, this sheet enables users to generate various types of visual analytics, such as compliance level distributions, gap analyses, and more.

By understanding the functionalities of these sheets, users can effectively navigate through the Excel Workbook and conduct a comprehensive DORA compliance assessment.

3.2 Instructions for Performing Compliance Assessment Using the Excel Workbook

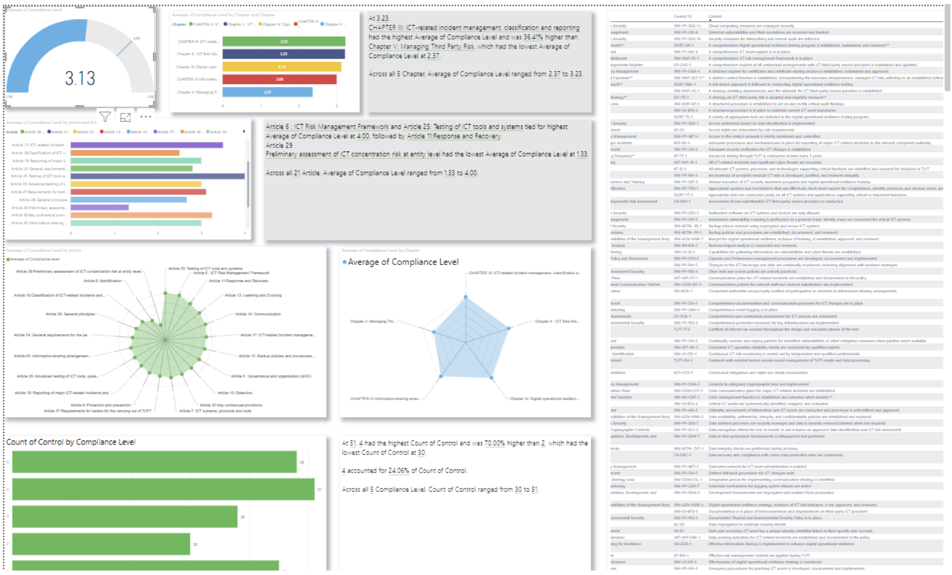
1. **Navigation to the 'Assessment' Sheet**:
   - Upon opening the Excel Workbook titled “WCS_DORA-(EU) 2022_2554_Compliance Assessment Template_v1.0”, the sheet labelled 'Assessment' is to be located. This sheet is designated as the primary interface where the compliance assessment is to be executed.

2. **Evaluation of Compliance Levels for Controls**:
    - In the 'Assessment' Sheet, a list of various controls is presented. For each listed control, the organization's current capabilities are to be assessed.
    - The column labeled 'Compliance Level' is equipped with a dropdown menu for each control.
    - The dropdown menu is to be utilized for selecting a score, which is aligned with the compliance maturity scale outlined in the 'Control Maturity Level Scoring' tab.
3. **Justification Provision**:
    - Subsequent to the selection of the compliance level, attention is to be directed to the adjacent 'Justification' column.
    - Supporting evidence or reasoning that substantiates the selected compliance level is to be entered here. This could encompass documentation, test results, or other forms of substantiating material.
4. **Gap Identification**:
    - The column labeled 'Gaps Identified' is to be navigated to next.
    - Any deficiencies or areas where the control does not meet full compliance are to be noted here. This assists in pinpointing areas necessitating improvement.
5. **Utilization of the Visualization Sheet for Graphical Insights**:
    - For obtaining a graphical interpretation and more in-depth insights into compliance levels, the 'Visualization Sheet' is to be accessed.
    - This sheet has been normalized to ensure compatibility with Power BI.
    - The 'Visualization Sheet' is to be imported into a Power BI Dashboard for an enhanced analytical view, thereby aiding in informed decision-making.

By meticulously adhering to these guidelines, a thorough compliance assessment can be conducted, facilitating an understanding of both the current capabilities and areas requiring improvement within the organization.

4 Power BI

The Power BI Dashboard, titled "WCS_DORA-(EU) 2022_2554_Compliance Assessment Visualization Dashboard," serves as an advanced analytical tool designed to offer a comprehensive view of compliance levels. This dashboard is intended to complement the Excel Workbook by providing a more interactive and visually engaging way to interpret compliance data.


3.13
3.23
3.22
3.13
3.00
2.37
Average of Compliance Level
CHAPTER III: ICT-related incident management, classification a...
Chapter V: Managing Thi...
Chapter II : ICT Risk Ma...
CHAPTER VI Information-sharing arran...
Chapter IV: Digital operational resilienc...
Count of Control by Compliance Level
51

At 3.23,
CHAPTER III: ICT-related incident management, classification and reporting had the highest Average of Compliance Level and was 36.41% higher than Chapter V: Managing Third Party Risk, which had the lowest Average of Compliance Level at 2.37.

Across all 5 Chapter, Average of Compliance Level ranged from 2.37 to 3.23.

Article 6 : ICT Risk Management Framework and Article 25: Testing of ICT tools and systems tied for highest Average of Compliance Level at 4.00, followed by Article 11:Response and Recovery.
Article 29
Preliminary assessment of ICT concentration risk at entity level had the lowest Average of Compliance Level at 1.33.

Across all 21 Article, Average of Compliance Level ranged from 1.33 to 4.00.

At 51, 4 had the highest Count of Control and was 70.00% higher than 2, which had the lowest Count of Control at 30.

4 accounted for 24.06% of Count of Control.

Across all 5 Compliance Level, Count of Control ranged from 30 to 51.

Figure 6 Power BI Dashboard

4.1 Accessing the Dashboard:

Upon launching Power BI, the dashboard titled "WCS_DORA-(EU) 2022_2554_Compliance Assessment Visualization Dashboard" is to be located and accessed.

Open **Power BI Desktop Application**, Go to **File**, Click on **Import** or **Open Report** and Select **Power BI Template >**

‘WCS_DORA-(EU) 2022_2554_Compliance Assessment Visualization Dashboard.pbix’

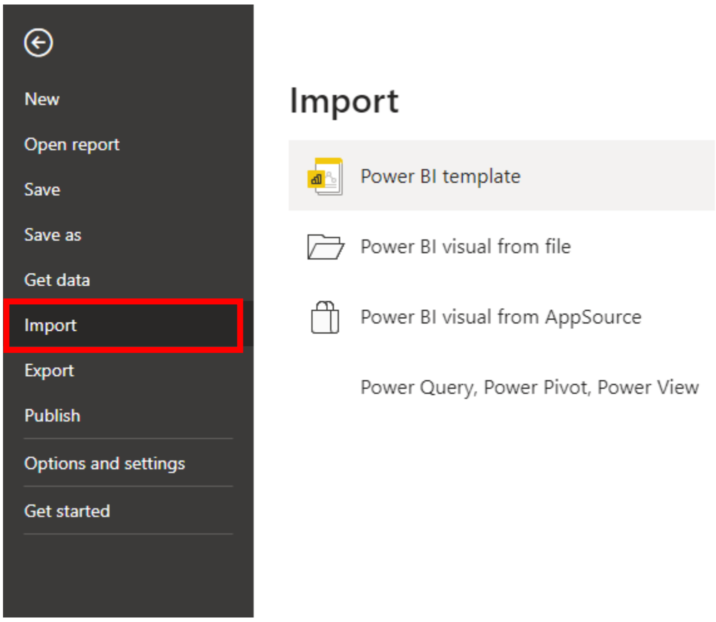


Figure 7 Importing Power BI Assessment Template

.

4.2 Importing Data from the Excel Workbook:

Upon initial access, the dashboard will display a sample assessment complete with its metrics. To update this with new data, the 'Visualization Sheet' from the Excel Workbook is to be imported. This sheet has been specifically normalized to ensure compatibility with Power BI. Importing this data will replace the sample assessment, thereby reflecting the most up-to-date compliance assessment metrics.

On the **ribbon**, click **on Excel Workbook** to Import a new Assessment excel to the Dashboard.

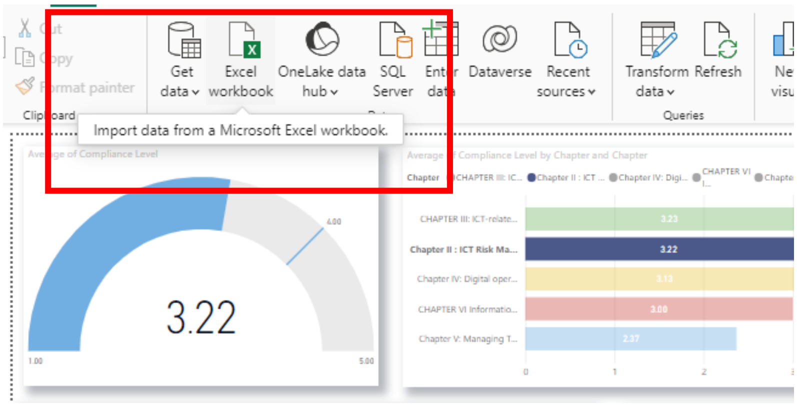
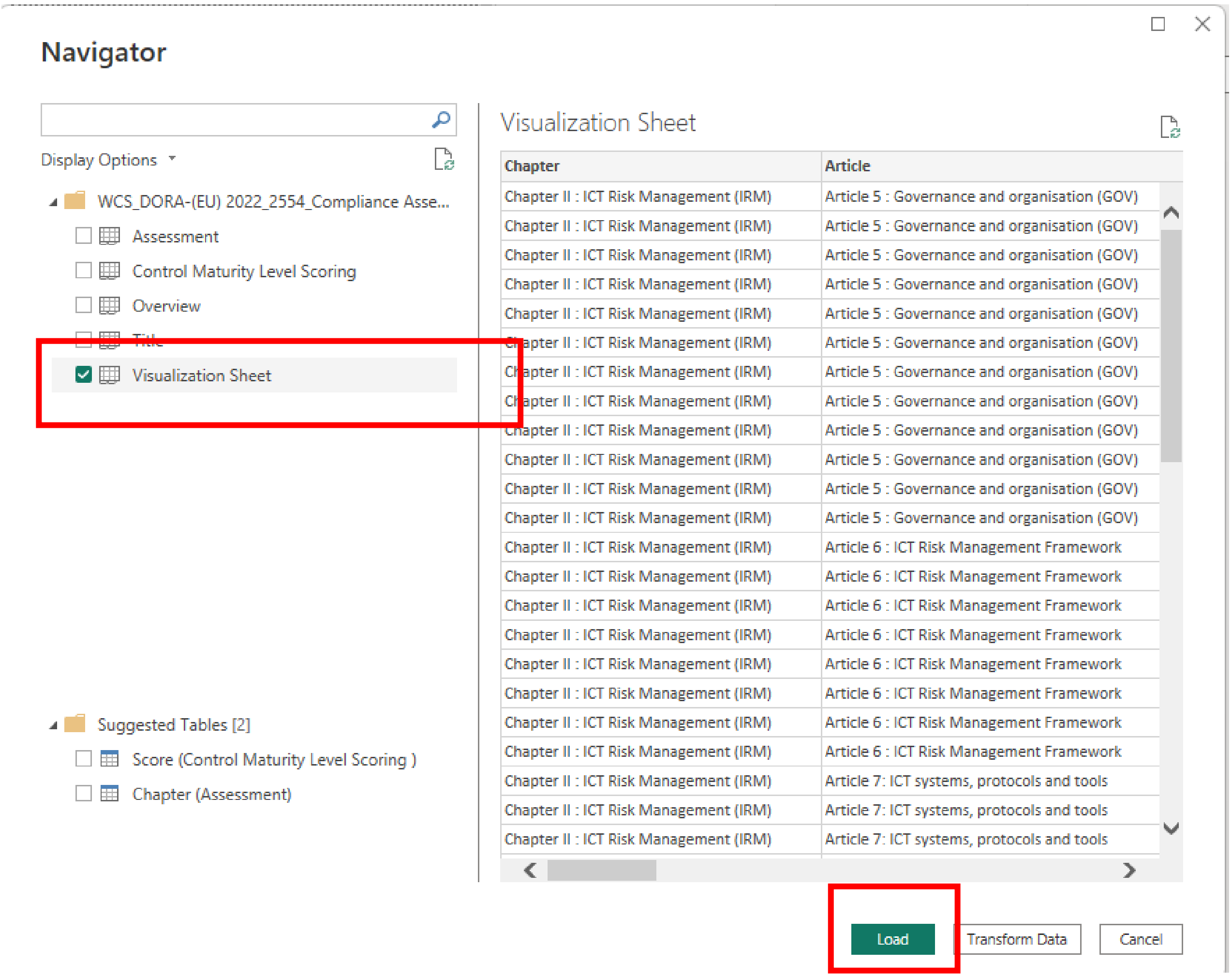


Figure 8 Importing A New Excel

Select the Assessment Excel Workbook, and in Select the **Visualization Sheet** as show in the figure below and click on **Load**.

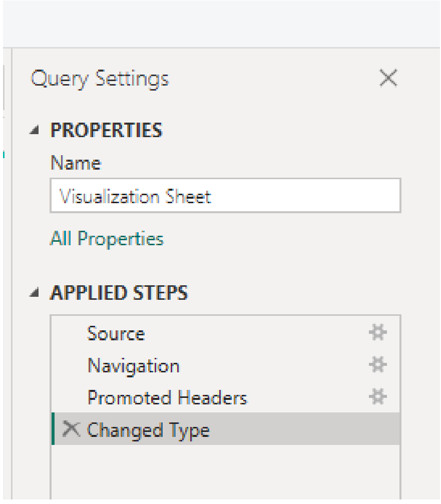


Visualization Sheet

Chapter	Article
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 6 : ICT Risk Management Framework
Chapter II : ICT Risk Management (IRM)	Article 7: ICT systems, protocols and tools
Chapter II : ICT Risk Management (IRM)	Article 7: ICT systems, protocols and tools
Chapter II : ICT Risk Management (IRM)	Article 7: ICT systems, protocols and tools

Figure 9 Loading Visualization Sheet

Make sure in the Transform Data, the Applied steps are followed as per the below properties, otherwise, there can be a connection issue between the visualization sheet and the dashboards.



Query Settings

PROPERTIES

Name

Visualization Sheet

All Properties

APPLIED STEPS

Source

Navigation

Promoted Headers

Changed Type

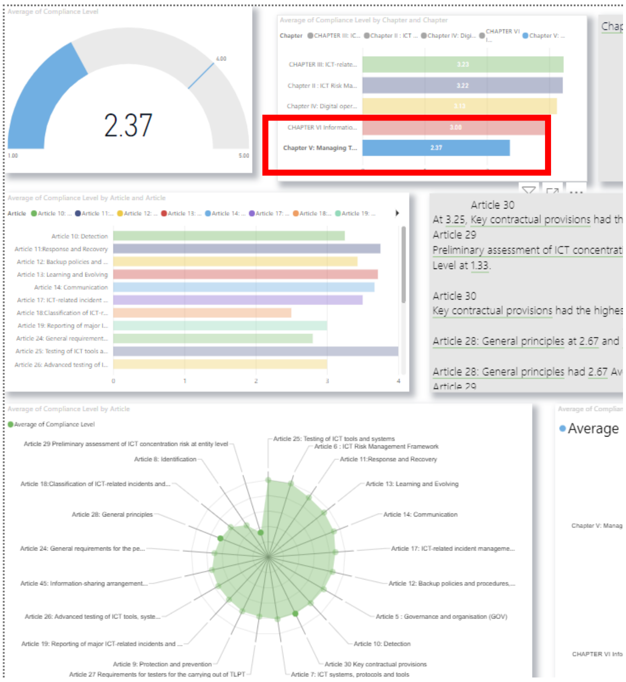
Figure 10 Table Properties

4.3 Dashboard Layout and Components

Once the dashboard is accessed, various visual components such as charts, graphs, and tables are presented. Each of these components is designed to offer specific insights into different aspects of compliance.

4.4 Interacting with Visual Components

The visual components are interactive and can be clicked on to drill down into more detailed data. This feature is to be utilized for gaining deeper insights into specific areas of compliance.


Average of Compliance Level
2.37
1.00
4.00
5.00
Average of Compliance Level by Chapter and Chapter
Chapter
CHAPTER III: IC...
Chapter II : ICT ...
Chapter IV: Digi...
CHAPTER VI I...
Chapter V: ...
CHAPTER III: ICT-relate...
Chapter II : ICT Risk Ma...
Chapter IV: Digital oper...
CHAPTER VI Informatio...
Chapter V: Managing T...
3.23
3.22
3.13
3.00
2.37
Average of Compliance Level by Article and Article
Article 10: Detection
Article 11:Response and Recovery
Article 12: Backup policies and ...
Article 13: Learning and Evolving
Article 14: Communication
Article 17: ICT-related incident ...
Article 18:Classification of ICT-r...
Article 19: Reporting of major I...
Article 24: General requirement...
Article 25: Testing of ICT tools a...
Article 26: Advanced testing of I...
0
1
2
3
4
Average of Compliance Level by Article
Average of Compliance Level
Average
Chapter V: Manag
CHAPTER VI Info

Article 30
At 3.25, Key contractual provisions had th
Article 29
Preliminary assessment of ICT concentrati
Level at 1.33.

Article 30
Key contractual provisions had the highes

Article 28: General principles at 2.67 and

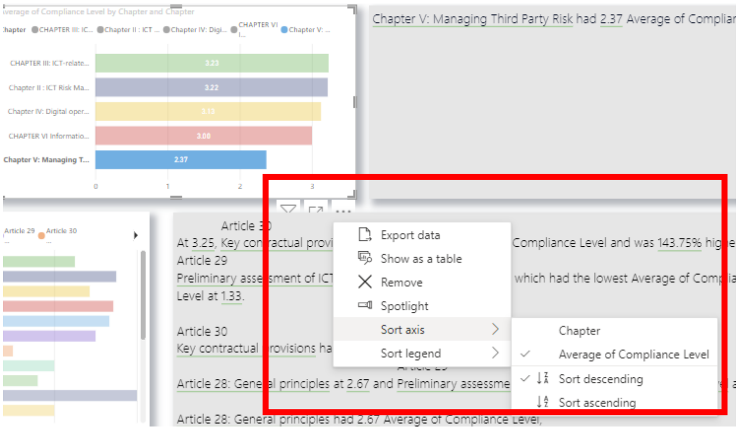
Article 28: General principles had 2.67 Av
Article 29

Figure 11 Interactive Dashboard Capabilities

Here, in the figure above, while selecting the Chapter V, all chart, graphs and insights are updated as to provide insight into that specific Chapter.

4.5 Filtering and Sorting Options

Filters and sorting options are available on the dashboard. These are to be used for customizing the view and focusing on particular aspects of the compliance data.



Chapter V: Managing Third Party Risk had 2.37 Average of Complian

Article 30

At 3.25, Key con ractual provi Compliance Level and was 143.75% hig e

Article 29

Preliminary asse sment of ICT which had the lowest Average of Comp ia

Level at 1.33.

Article 30

Key contractual rovisions ha

Article 28: Gene al principles at 2.67 and Preliminary assessme

Article 28: General principles had 2.67 Average of Compliance Level,

Figure 12 Sorting and Filtering Capabilities

4.6 Exporting Reports

If a hard copy of the dashboard or specific components is required, the export option is to be used. This allows for the generation of reports in various formats such as PDF or Power BI template. To Export, Click on File, and Select Export Option.

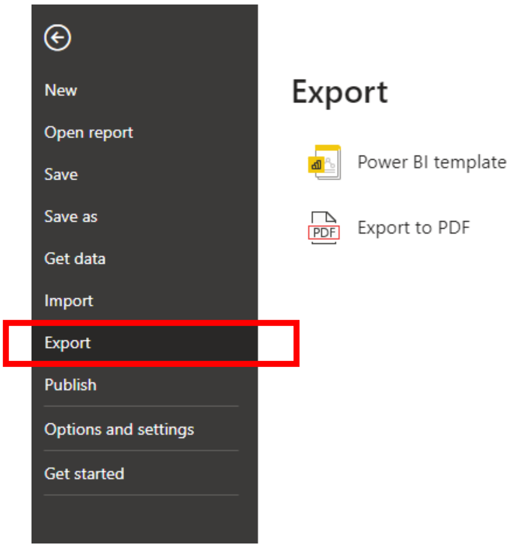


Figure 13 Export Options

4.7 Updating the Dashboard

To ensure that the dashboard remains current, it is advisable to regularly update it by re-importing the 'Visualization Sheet' from the Excel Workbook whenever new assessment data is available.

By following these guidelines, a comprehensive and interactive view of the organization's compliance status can be obtained. This facilitates not only a better understanding of current compliance levels but also aids in identifying areas that may require further attention or improvement.

5 OneTrust Platform Compliance Assessment Template

5.1 Accessing and Editing the Template

1. **Initial Access**: To access the OneTrust DORA Pre-Readiness Compliance Assessment Template, users must first log in to the OneTrust portal using the link : https://app-de.onetrust.com/auth/login.

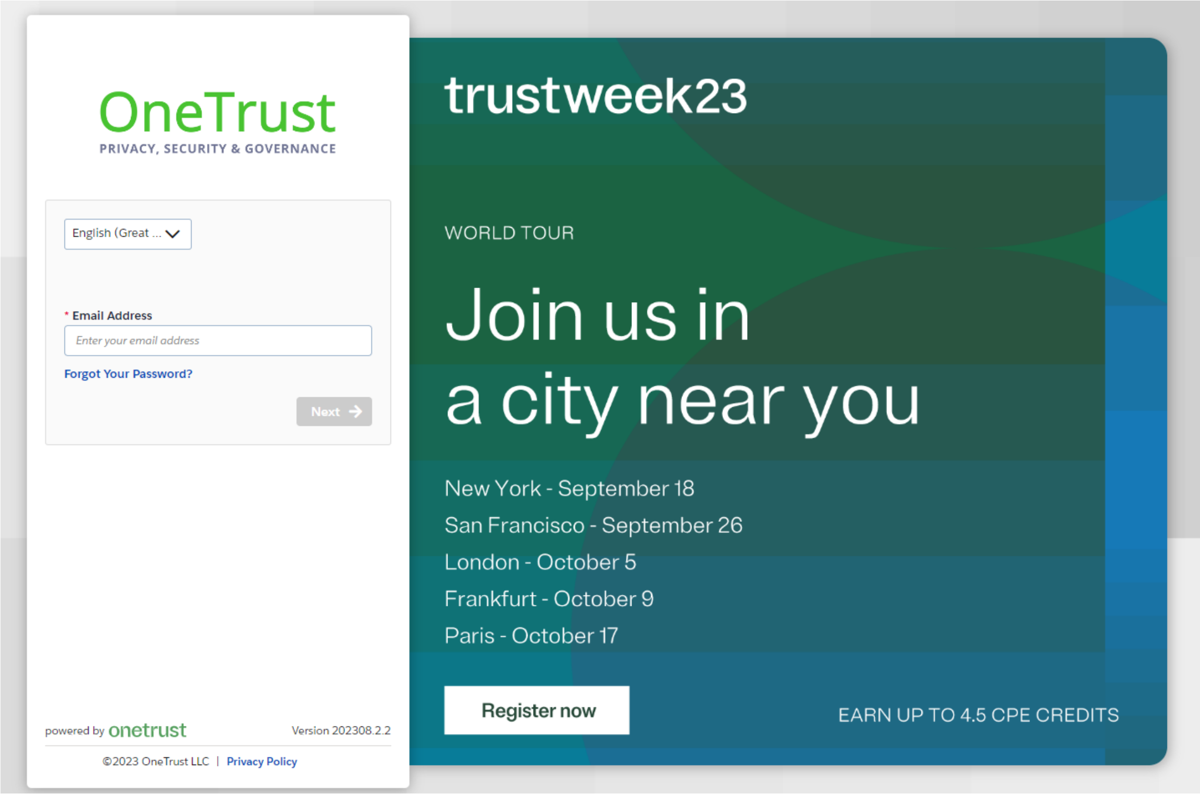


Figure 14 One Trust Login

2. **Navigating to Template**: Once logged in, select 'Third-Party Risk Management' and navigate to the 'Setup' section. Here, the templates are listed. Select DORA Pre-Readiness Compliance Assessment Template.

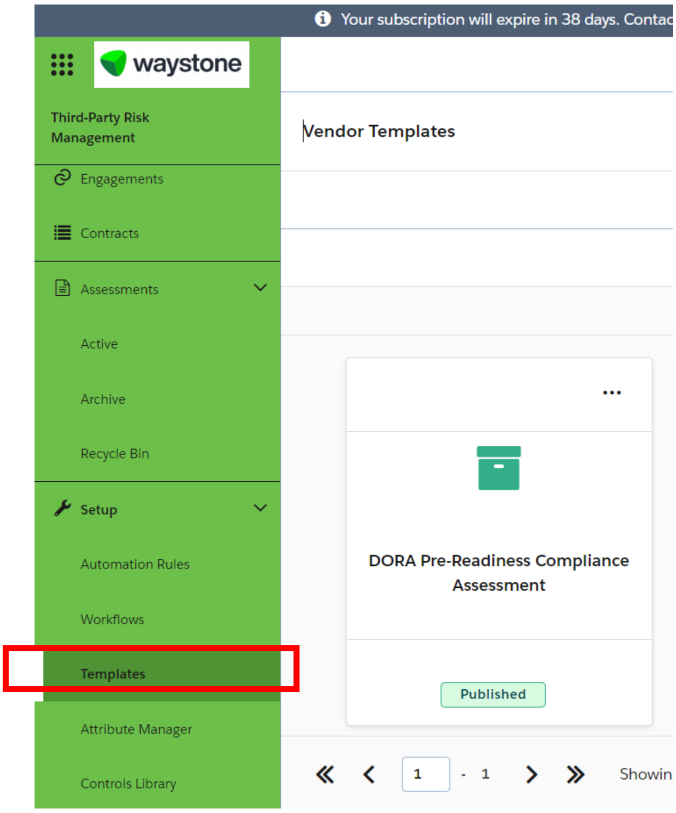
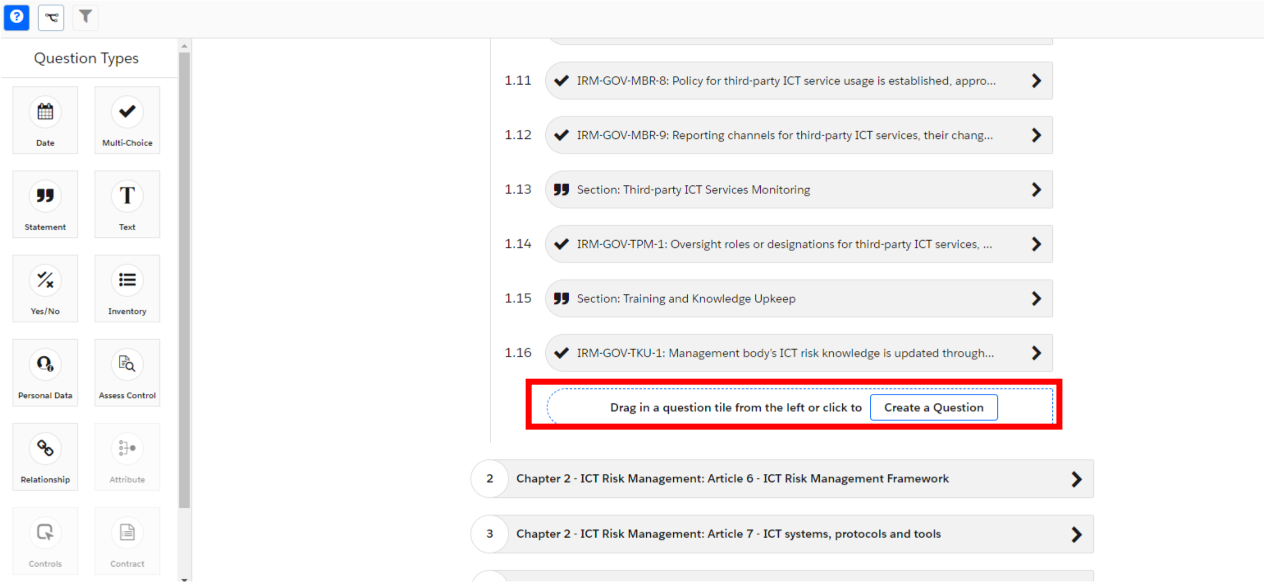


Figure 15 DORA Template Location

3. **Editing the Template**: To modify the existing template or add new sections/controls, click on the 'Add Section' or 'Add Question' buttons, respectively. This allows for customization of the template to suit specific needs.

   Steps Performed to Develop a Control

- **Question Type - Multi-Choice**: To develop a control within a section, the "multi-Choice" question type is selected.
- **Question Naming**: The name of the question is set to match the Control ID and description from the Control Database. For example, the question might be named "IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed."
- **Control Description**: The description for each control, as outlined in the Control Database, is pasted into the question's description field.
- **Question Hint and Recommendations**: The "Question Hint" feature is enabled, and recommendations for achieving compliance are added. This serves as a guide for the assessor.
- **Allow Justification**: The "Allow Justification" feature is enabled. This allows the assessor to provide justifications for the scores they assign, as well as to identify any gaps in compliance.
- **Scoring Options**: The Multi-Choice options are set to range from 1 to 5, corresponding to the compliance level. Each number is defined according to the scoring methodology, allowing for a nuanced evaluation of compliance.



1.11 IRM-GOV-MBR-8: Policy for third-party ICT service usage is established, appro...

1.12 IRM-GOV-MBR-9: Reporting channels for third-party ICT services, their chang...

1.13 Section: Third-party ICT Services Monitoring

1.14 IRM-GOV-TPM-1: Oversight roles or designations for third-party ICT services, ...

1.15 Section: Training and Knowledge Upkeep

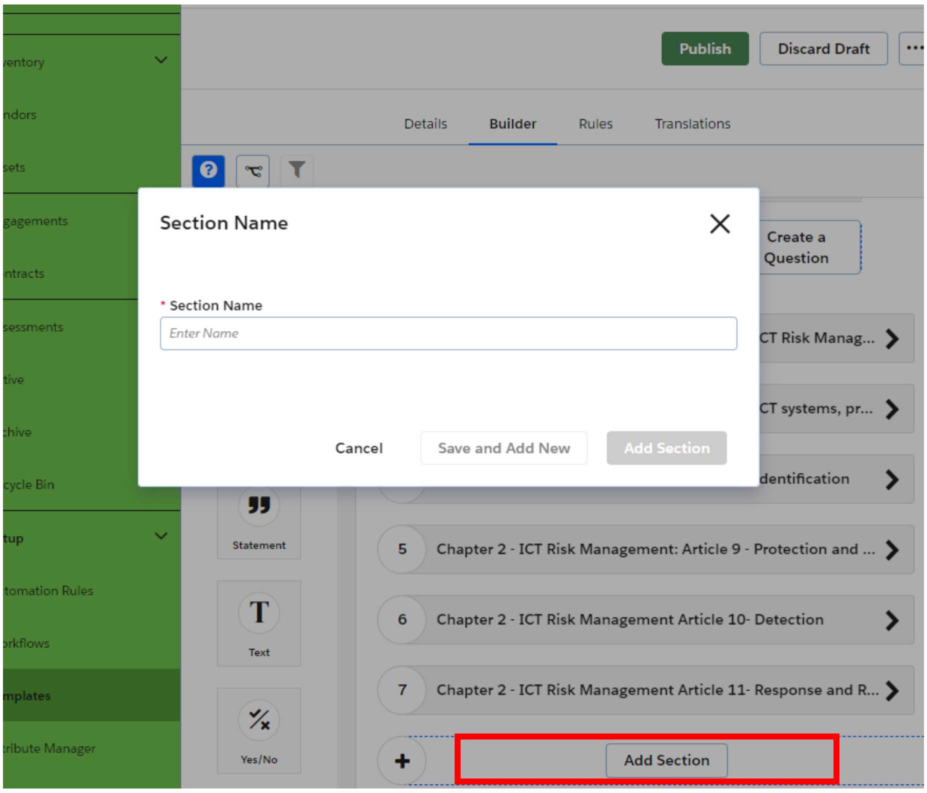
1.16 IRM-GOV-TKU-1: Management body's ICT risk knowledge is updated through...

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

2 Chapter 2 - ICT Risk Management: Article 6 - ICT Risk Management Framework

3 Chapter 2 - ICT Risk Management: Article 7 - ICT systems, protocols and tools

Figure 16 Adding New Controls



Section Name

* Section Name

Enter Name

Cancel   Save and Add New   Add Section

CT Risk Manag...

CT systems, pr...

dentification

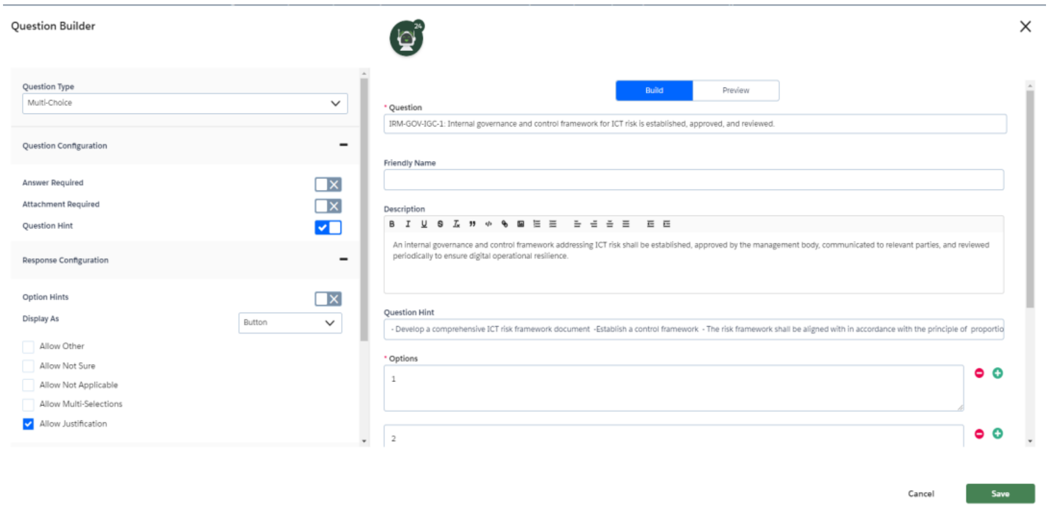
5 Chapter 2 - ICT Risk Management: Article 9 - Protection and ...

6 Chapter 2 - ICT Risk Management Article 10- Detection

7 Chapter 2 - ICT Risk Management Article 11- Response and R...

Add Section

Figure 17 Adding New Sections



Question Builder

Question Type: Multi-Choice

Question Configuration

Answer Required ☒

Attachment Required ☒

Question Hint ☑

Response Configuration

Option Hints ☒

Display As: Button

□ Allow Other

□ Allow Not Sure

□ Allow Not Applicable

□ Allow Multi-Selections

☑ Allow Justification

* Question: IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed.

Friendly Name:

Description: An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.

Question Hint: - Develop a comprehensive ICT risk framework document -Establish a control framework - The risk framework shall be aligned with in accordance with the principle of proportio

* Options

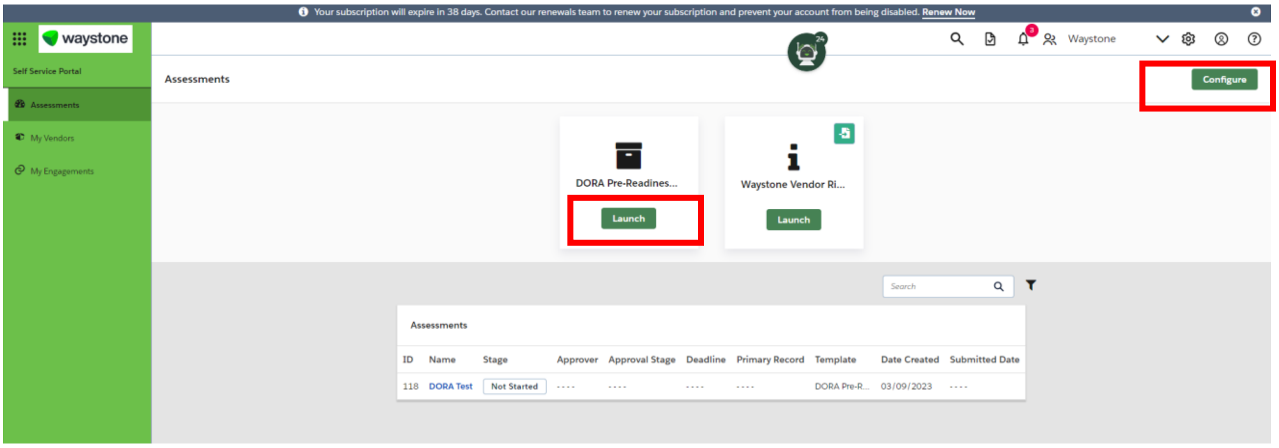
1

2

Figure 18 Question Builder

5.2 Performing the Assessment:

1. **Starting the Assessment**: To initiate the assessment, go to the self-service portal within the OneTrust portal. Configure the published DORA Template and click 'Launch' to begin.



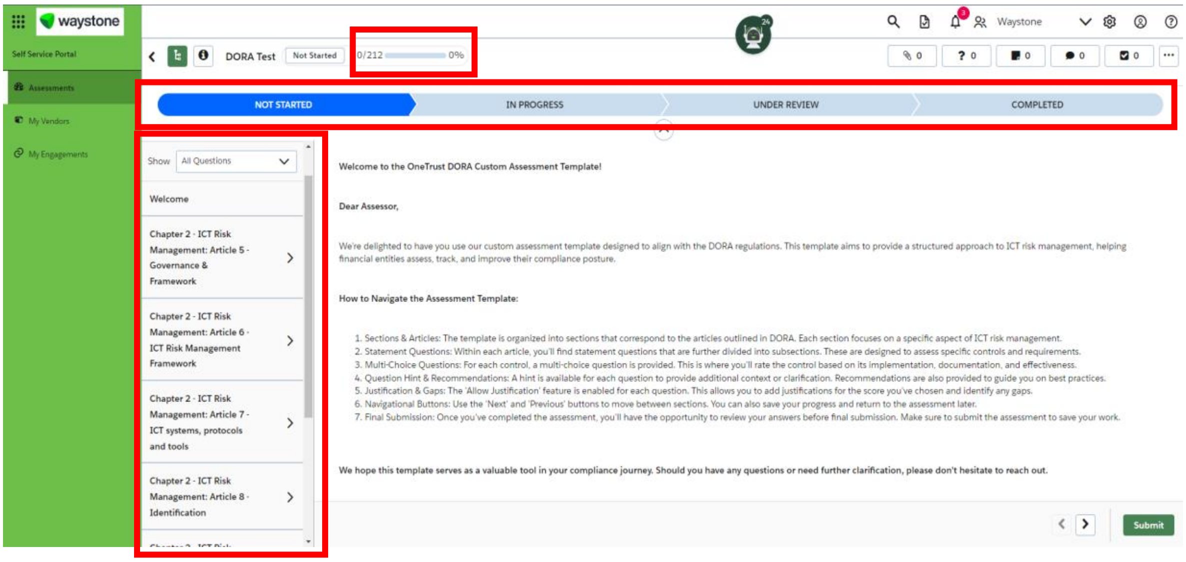
Your subscription will expire in 38 days. Contact our renewals team to renew your subscription and prevent your account from being disabled. Renew Now

Assessments

ID	Name	Stage	Approver	Approval Stage	Deadline	Primary Record	Template	Date Created	Submitted Date
118	DORA Test	Not Started	----	----	----	----	DORA Pre-R...	03/09/2023	----

Figure 19 Starting Assessment

2. **Welcome Screen**: Upon launching, a welcome screen appears, providing instructions for navigating through the assessment.


waystone
Self Service Portal
Assessments
My Vendors
My Engagements
DORA Test
Not Started
0/212
0%
Waystone
NOT STARTED
IN PROGRESS
UNDER REVIEW
COMPLETED
Show
All Questions
Welcome
Chapter 2 - ICT Risk Management: Article 5 - Governance & Framework
Chapter 2 - ICT Risk Management: Article 6 - ICT Risk Management Framework
Chapter 2 - ICT Risk Management: Article 7 - ICT systems, protocols and tools
Chapter 2 - ICT Risk Management: Article 8 - Identification
Submit

Welcome to the OneTrust DORA Custom Assessment Template!

Dear Assessor,

We're delighted to have you use our custom assessment template designed to align with the DORA regulations. This template aims to provide a structured approach to ICT risk management, helping financial entities assess, track, and improve their compliance posture.

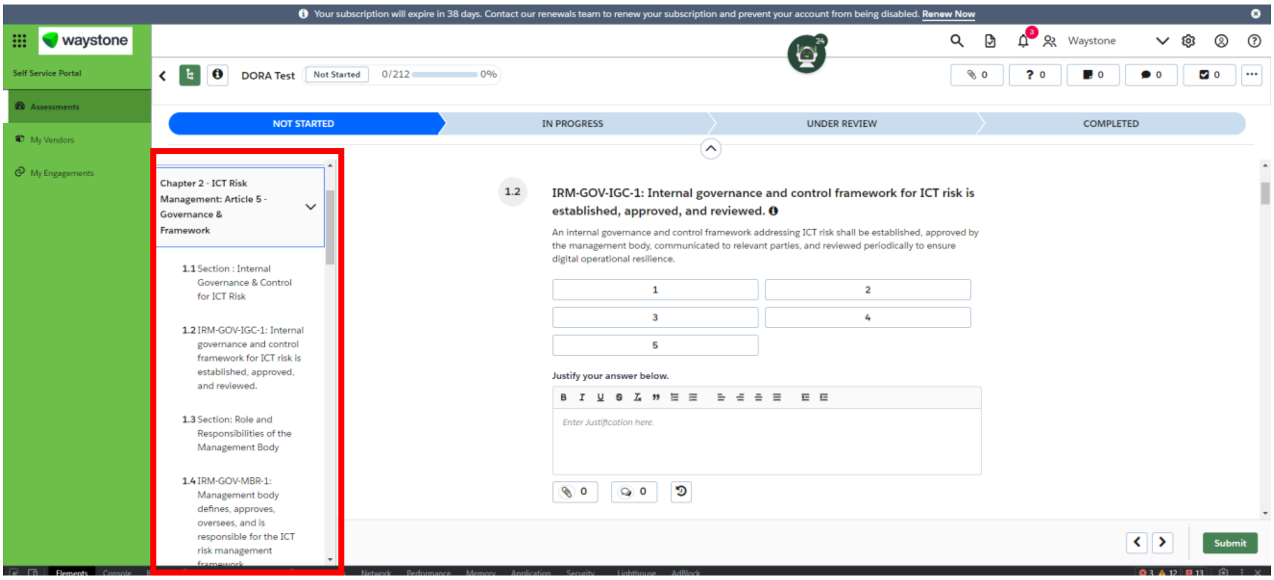
How to Navigate the Assessment Template:

1. Sections & Articles: The template is organized into sections that correspond to the articles outlined in DORA. Each section focuses on a specific aspect of ICT risk management.
2. Statement Questions: Within each article, you'll find statement questions that are further divided into subsections. These are designed to assess specific controls and requirements.
3. Multi-Choice Questions: For each control, a multi-choice question is provided. This is where you'll rate the control based on its implementation, documentation, and effectiveness.
4. Question Hint & Recommendations: A hint is available for each question to provide additional context or clarification. Recommendations are also provided to guide you on best practices.
5. Justification & Gaps: The 'Allow Justification' feature is enabled for each question. This allows you to add justifications for the score you've chosen and identify any gaps.
6. Navigational Buttons: Use the 'Next' and 'Previous' buttons to move between sections. You can also save your progress and return to the assessment later.
7. Final Submission: Once you've completed the assessment, you'll have the opportunity to review your answers before final submission. Make sure to submit the assessment to save your work.

We hope this template serves as a valuable tool in your compliance journey. Should you have any questions or need further clarification, please don't hesitate to reach out.

Figure 20 Welcome Screen

3. **Navigating Through Articles**: On the left-hand side, various articles are listed. Clicking on an article will display questions for each section under that article as shown in figure 20 & 21.


Your subscription will expire in 38 days. Contact our renewals team to renew your subscription and prevent your account from being disabled. Renew Now
waystone
Self Service Portal
Assessments
My Vendors
My Engagements
DORA Test
Not Started
0/212
0%
Waystone
NOT STARTED
IN PROGRESS
UNDER REVIEW
COMPLETED
Chapter 2 - ICT Risk Management: Article 5 - Governance & Framework
1.1 Section : Internal Governance & Control for ICT Risk
1.2 IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed.
1.3 Section: Role and Responsibilities of the Management Body
1.4 IRM-GOV-MBR-1: Management body defines, approves, oversees, and is responsible for the ICT risk management framework
Submit

1.2 IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed.

An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.

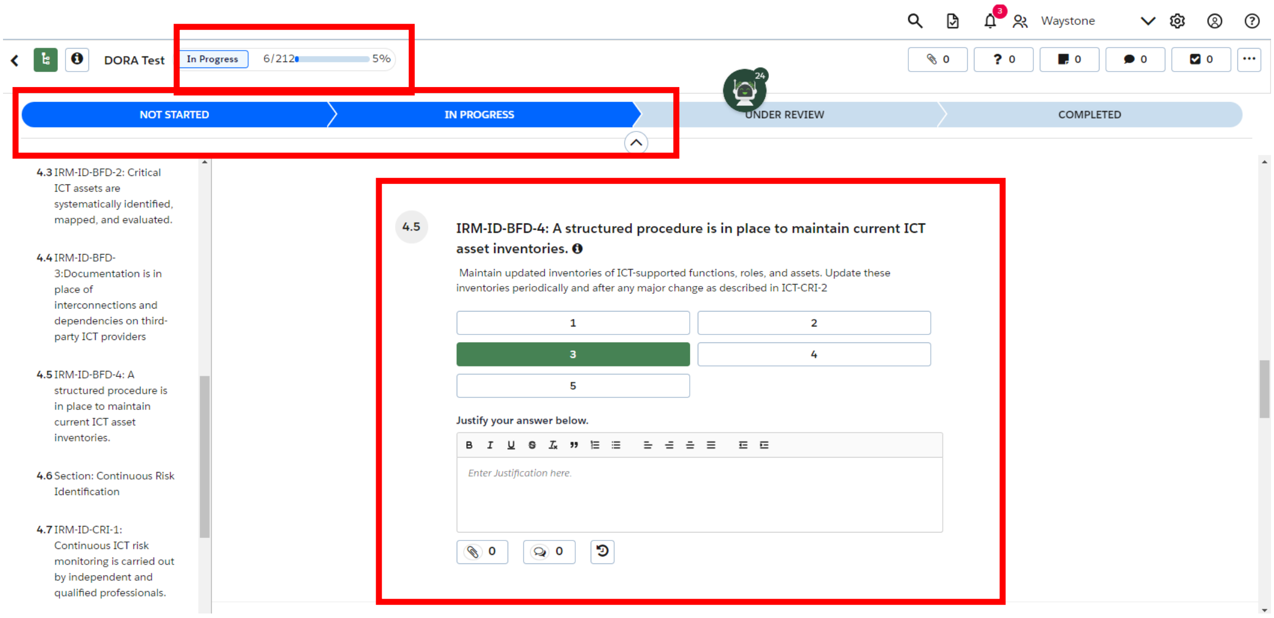
1	2
3	4
5	

Justify your answer below.

Enter Justification here.

Figure 21 Navigating the Controls

4. **Assessment Start and Status**: The status of the assessment changes from 'Not Started' to 'In Progress' once a compliance control level is selected for any of the controls. Select the compliance control by level by simply selecting the options present.



4.3 IRM-ID-BFD-2: Critical ICT assets are systematically identified, mapped, and evaluated.

4.4 IRM-ID-BFD-3:Documentation is in place of interconnections and dependencies on third-party ICT providers

4.5 IRM-ID-BFD-4: A structured procedure is in place to maintain current ICT asset inventories.

4.6 Section: Continuous Risk Identification

4.7 IRM-ID-CRI-1: Continuous ICT risk monitoring is carried out by independent and qualified professionals.

4.5 IRM-ID-BFD-4: A structured procedure is in place to maintain current ICT asset inventories.

Maintain updated inventories of ICT-supported functions, roles, and assets. Update these inventories periodically and after any major change as described in ICT-CRI-2

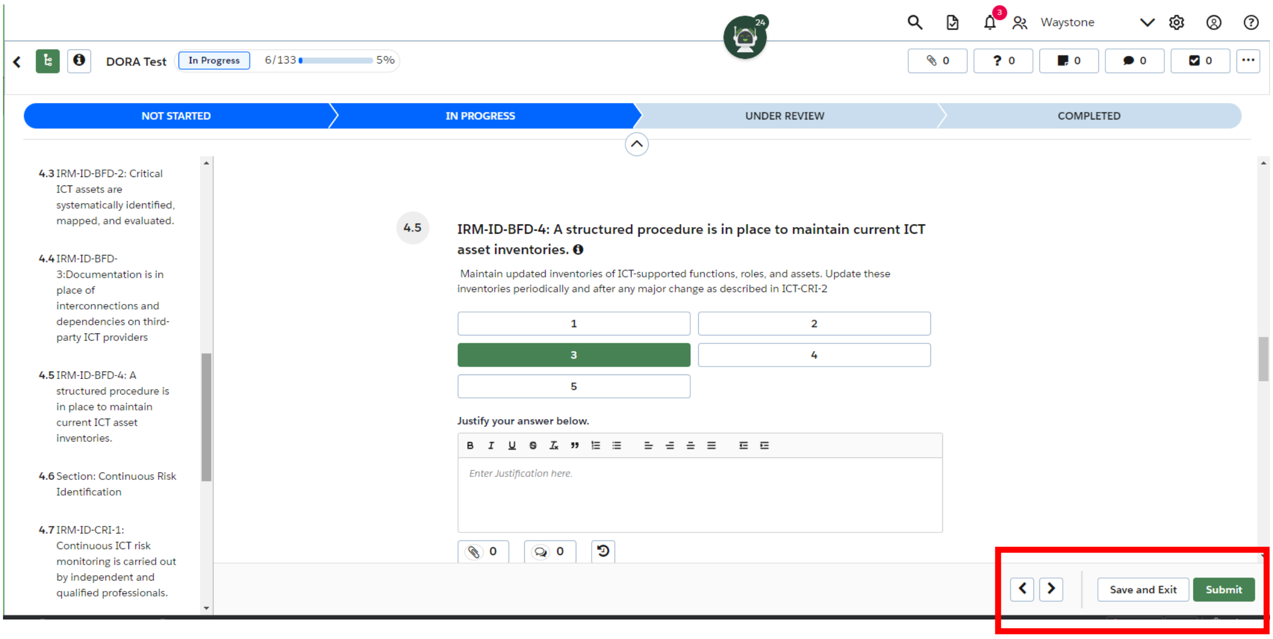
Justify your answer below.

Enter Justification here.

Figure 22 Evaluation of Controls

5. **Progress Tracking**: On the top-left corner of the dashboard, a status bar shows the total number of controls and the number of controls that have been assessed. As highlighted in figure 22, top left.

6. **Completion and Review**: Once the assessment is complete, click 'Submit' at the bottom left. This will share the assessment with the reviewer and change the status from 'In Progress' to 'Under Review'. The reviewer can then review the entire assessment and, upon completion, click 'Finish Review' at the bottom left. This will change the status to 'Completed'.



4.3 IRM-ID-BFD-2: Critical ICT assets are systematically identified, mapped, and evaluated.

4.4 IRM-ID-BFD-3:Documentation is in place of interconnections and dependencies on third-party ICT providers

4.5 IRM-ID-BFD-4: A structured procedure is in place to maintain current ICT asset inventories.

4.6 Section: Continuous Risk Identification

4.7 IRM-ID-CRI-1: Continuous ICT risk monitoring is carried out by independent and qualified professionals.

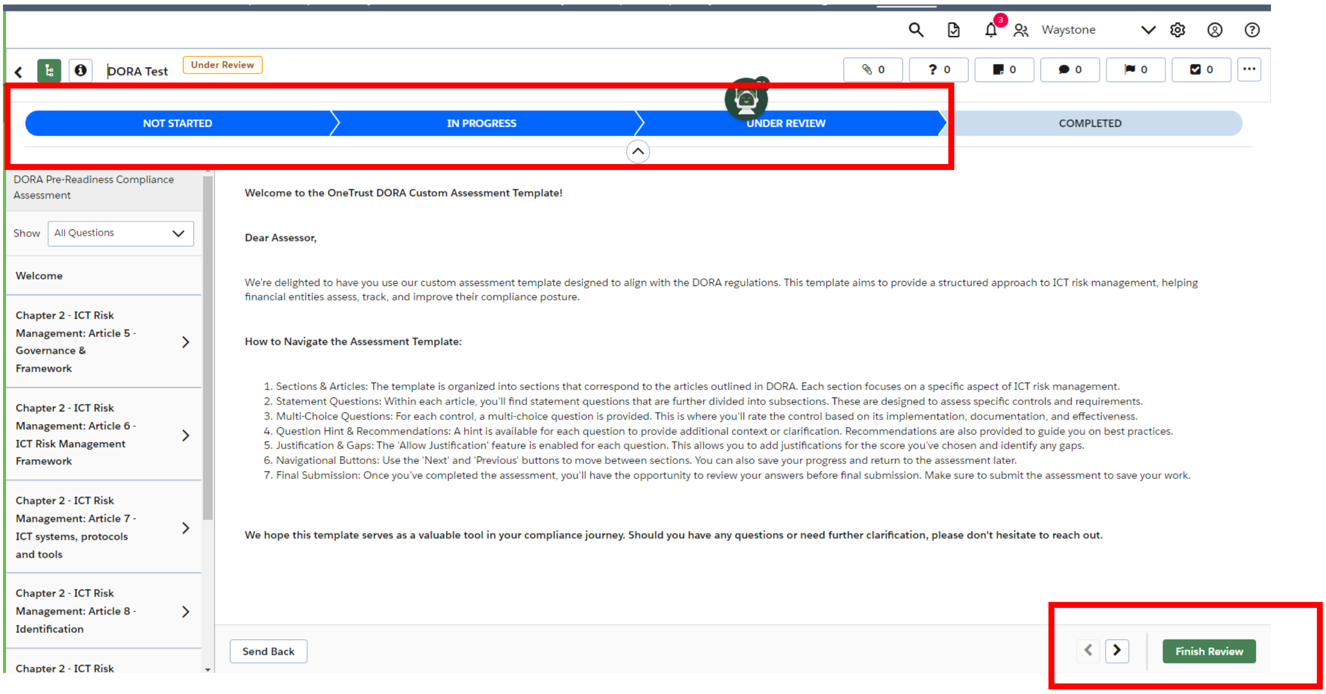
4.5 IRM-ID-BFD-4: A structured procedure is in place to maintain current ICT asset inventories.

Maintain updated inventories of ICT-supported functions, roles, and assets. Update these inventories periodically and after any major change as described in ICT-CRI-2

Justify your answer below.

Enter Justification here.

Figure 23 Submitting the Assessment



Waystone
DORA Test
Under Review
NOT STARTED
IN PROGRESS
UNDER REVIEW
COMPLETED
DORA Pre-Readiness Compliance Assessment
Show
All Questions
Welcome
Chapter 2 - ICT Risk Management: Article 5 - Governance & Framework
Chapter 2 - ICT Risk Management: Article 6 - ICT Risk Management Framework
Chapter 2 - ICT Risk Management: Article 7 - ICT systems, protocols and tools
Chapter 2 - ICT Risk Management: Article 8 - Identification
Chapter 2 - ICT Risk
Send Back
Finish Review

Welcome to the OneTrust DORA Custom Assessment Template!

Dear Assessor,

We're delighted to have you use our custom assessment template designed to align with the DORA regulations. This template aims to provide a structured approach to ICT risk management, helping financial entities assess, track, and improve their compliance posture.

How to Navigate the Assessment Template:

1. Sections & Articles: The template is organized into sections that correspond to the articles outlined in DORA. Each section focuses on a specific aspect of ICT risk management.
2. Statement Questions: Within each article, you'll find statement questions that are further divided into subsections. These are designed to assess specific controls and requirements.
3. Multi-Choice Questions: For each control, a multi-choice question is provided. This is where you'll rate the control based on its implementation, documentation, and effectiveness.
4. Question Hint & Recommendations: A hint is available for each question to provide additional context or clarification. Recommendations are also provided to guide you on best practices.
5. Justification & Gaps: The 'Allow Justification' feature is enabled for each question. This allows you to add justifications for the score you've chosen and identify any gaps.
6. Navigational Buttons: Use the 'Next' and 'Previous' buttons to move between sections. You can also save your progress and return to the assessment later.
7. Final Submission: Once you've completed the assessment, you'll have the opportunity to review your answers before final submission. Make sure to submit the assessment to save your work.

We hope this template serves as a valuable tool in your compliance journey. Should you have any questions or need further clarification, please don't hesitate to reach out.

Figure 24 Finishing the Assessment

5.3 Exporting the Assessment:

1. **Export Options**: Various options are available for exporting the assessment results. Click on the three dots at the top right corner and select 'Export Responses' or 'Export as PDF'.
2. **Additional Features**: Other functionalities include importing responses using an Excel sheet and sending reminders to complete the assessment
3.

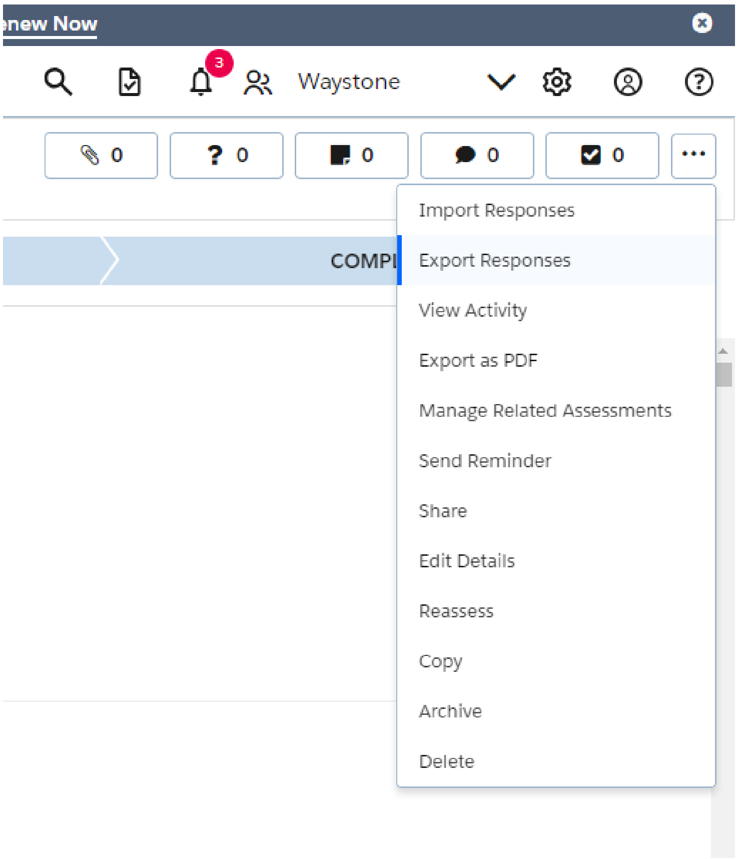
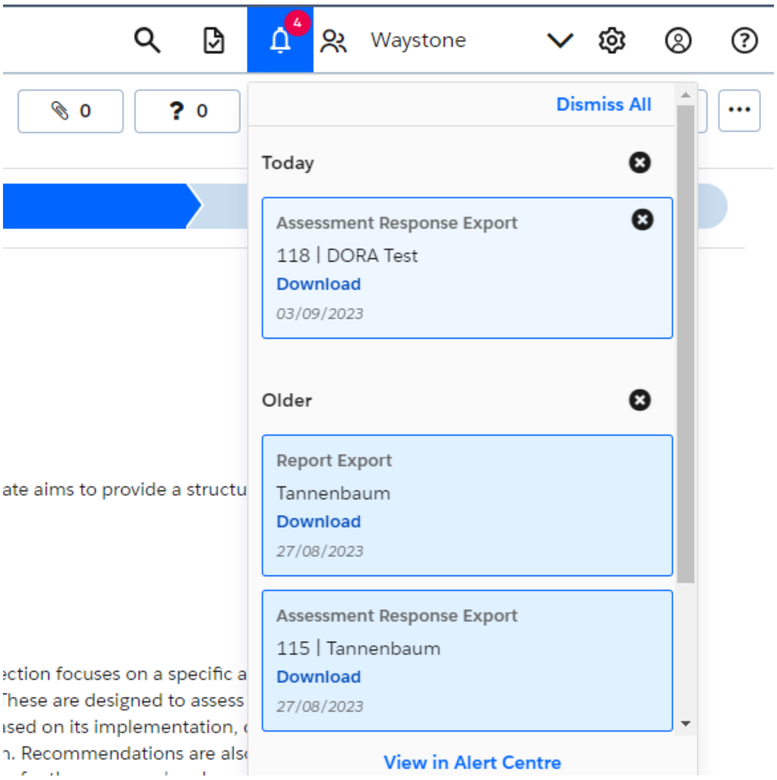


Figure 25 Using Export Options



Assessment Response Export
118 | DORA Test
Download
03/09/2023

Report Export
Tannenbaum
Download
27/08/2023

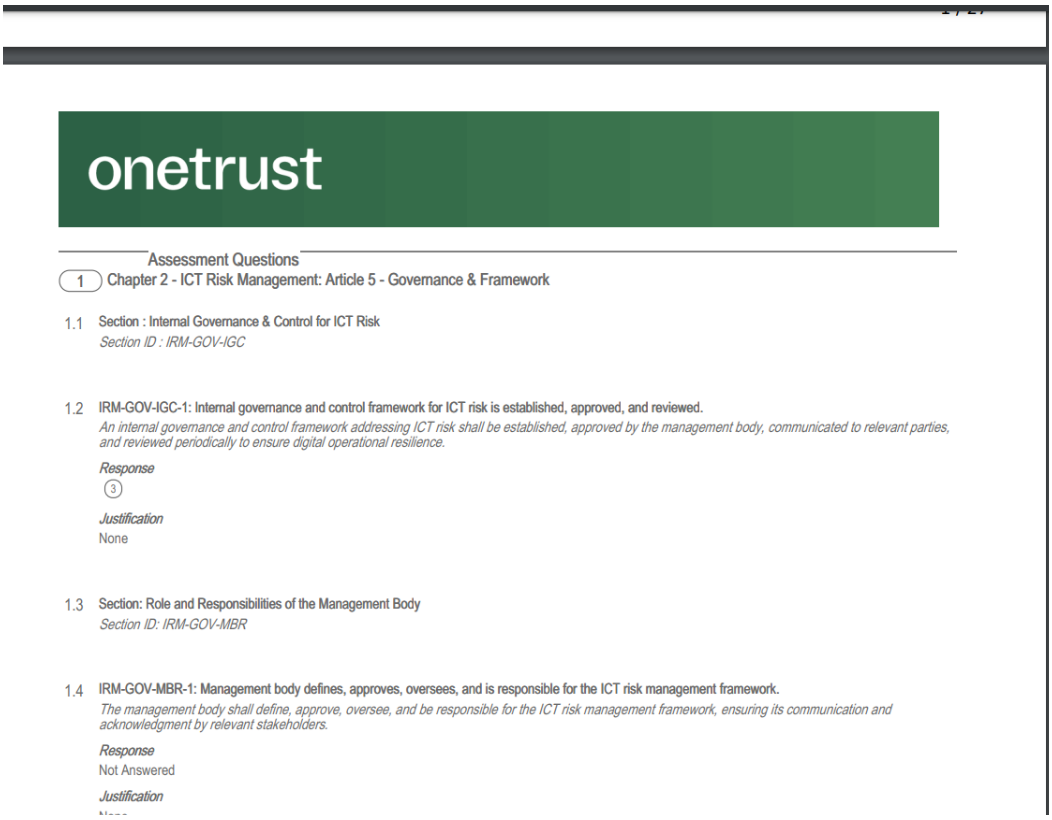
Assessment Response Export
115 | Tannenbaum
Download
27/08/2023

ate aims to provide a structu

ection focuses on a specific a
These are designed to assess
ased on its implementation,
n. Recommendations are als

4.

5. Figure 26 Downloading Exporting



Assessment Questions

1 Chapter 2 - ICT Risk Management: Article 5 - Governance & Framework

1.1 Section : Internal Governance & Control for ICT Risk
Section ID : IRM-GOV-IGC

1.2 IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed.
An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.

Response
3

Justification
None

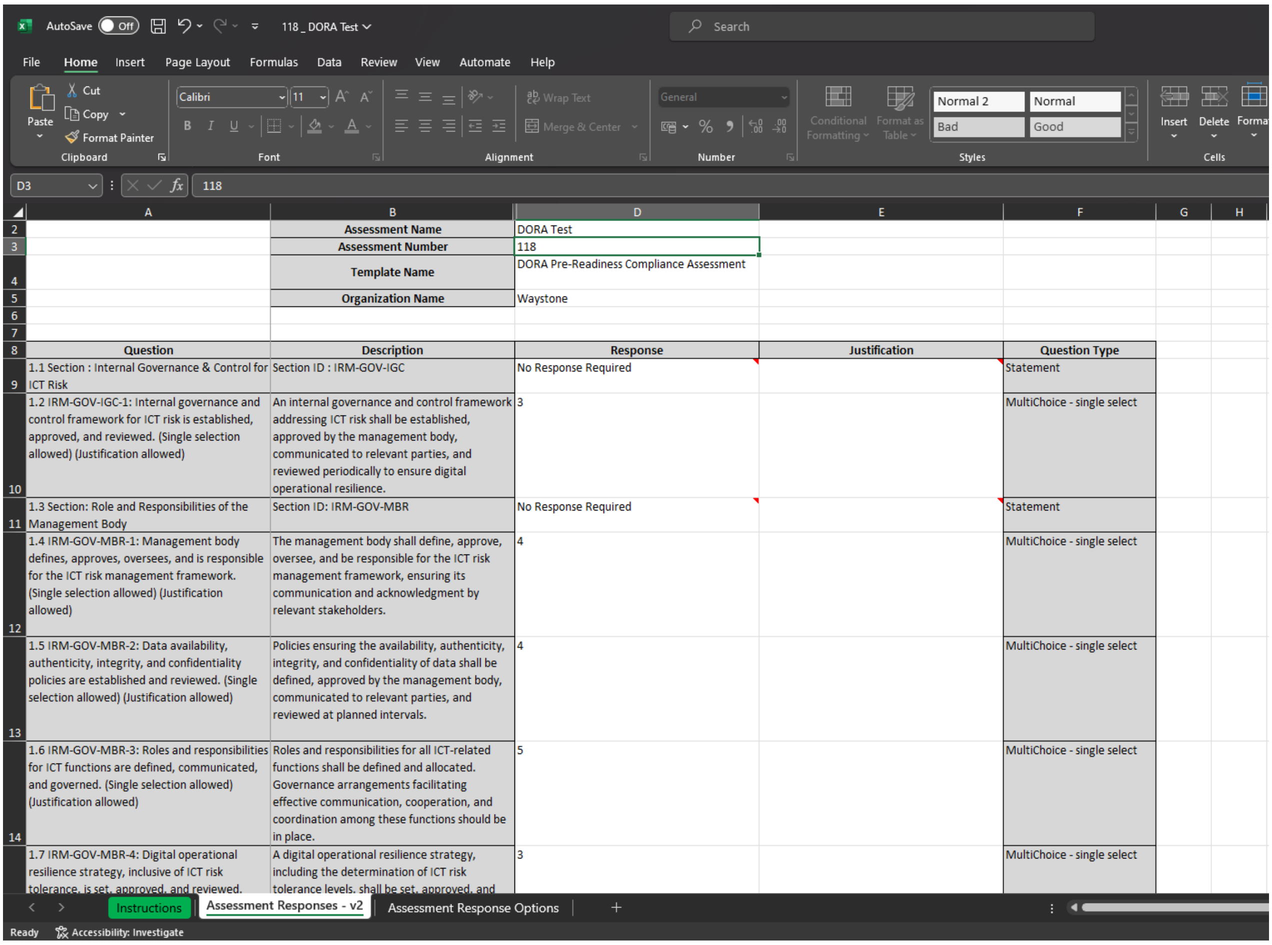
1.3 Section: Role and Responsibilities of the Management Body
Section ID: IRM-GOV-MBR

1.4 IRM-GOV-MBR-1: Management body defines, approves, oversees, and is responsible for the ICT risk management framework.
The management body shall define, approve, oversee, and be responsible for the ICT risk management framework, ensuring its communication and acknowledgment by relevant stakeholders.

Response
Not Answered

Justification

Figure 27 Sample Exported PDF



	A	B	D	E	F	G	H
2		Assessment Name	DORA Test				
3		Assessment Number	118				
4		Template Name	DORA Pre-Readiness Compliance Assessment				
5		Organization Name	Waystone				
6							
7							
8	Question	Description	Response	Justification	Question Type		
9	1.1 Section : Internal Governance & Control for ICT Risk	Section ID : IRM-GOV-IGC	No Response Required		Statement		
10	1.2 IRM-GOV-IGC-1: Internal governance and control framework for ICT risk is established, approved, and reviewed. (Single selection allowed) (Justification allowed)	An internal governance and control framework addressing ICT risk shall be established, approved by the management body, communicated to relevant parties, and reviewed periodically to ensure digital operational resilience.	3		MultiChoice - single select		
11	1.3 Section: Role and Responsibilities of the Management Body	Section ID: IRM-GOV-MBR	No Response Required		Statement		
12	1.4 IRM-GOV-MBR-1: Management body defines, approves, oversees, and is responsible for the ICT risk management framework. (Single selection allowed) (Justification allowed)	The management body shall define, approve, oversee, and be responsible for the ICT risk management framework, ensuring its communication and acknowledgment by relevant stakeholders.	4		MultiChoice - single select		
13	1.5 IRM-GOV-MBR-2: Data availability, authenticity, integrity, and confidentiality policies are established and reviewed. (Single selection allowed) (Justification allowed)	Policies ensuring the availability, authenticity, integrity, and confidentiality of data shall be defined, approved by the management body, communicated to relevant parties, and reviewed at planned intervals.	4		MultiChoice - single select		
14	1.6 IRM-GOV-MBR-3: Roles and responsibilities for ICT functions are defined, communicated, and governed. (Single selection allowed) (Justification allowed)	Roles and responsibilities for all ICT-related functions shall be defined and allocated. Governance arrangements facilitating effective communication, cooperation, and coordination among these functions should be in place.	5		MultiChoice - single select		
	1.7 IRM-GOV-MBR-4: Digital operational resilience strategy, inclusive of ICT risk tolerance, is set, approved, and reviewed.	A digital operational resilience strategy, including the determination of ICT risk tolerance levels, shall be set, approved, and	3		MultiChoice - single select		

Figure 28 Sample Exported Excel Responses

5.4 Appendix H – Monthly Internship Activity Report – Month 1

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Rishabh Sachdeva Student number: x21213909

Company: Waystone Compliance Solutions Month Commencing: June 2023

During the first month of my internship, a myriad of tasks and activities were undertaken to ensure both the primary and secondary objectives were met. The primary focus was on developing the Pre-Readiness Compliance Assessment Framework for DORA. This entailed a comprehensive review of existing literature to gain a nuanced understanding of the subject matter, followed by the formulation of a well-defined research introduction. Key research questions were identified, and clear objectives were set to guide the project. The research approach was also finalized during this period, providing the project with a clear and focused direction. By the end of the month, the initial stages of developing the control framework were set into motion. In addition to the primary research, I was also involved in several secondary tasks. One notable project was the development of an M365 Environment Configuration Analysis Script. This script, when executed, runs a series of configuration tools including Monkey365, Inspect365, and ScuBA. The output is a comprehensive dashboard that amalgamates insights from all these tools, offering a holistic view of the environment's configuration status. Furthermore, I engaged in client-specific tasks such as conducting a ransomware readiness assessment, which involved evaluating a client's vulnerability to ransomware attacks and providing actionable recommendations. Overall, the first month was a blend of research, development, and client engagement, laying a robust foundation for the remainder of the internship.

Employer comments

Rishabh has been an exceptional asset in his first month of internship. His work on the DORA framework has been thorough and insightful, setting a strong foundation for the project. Beyond that, his development of the M365 script and client-specific tasks like ransomware readiness assessments have been equally impressive. Rishabh's blend of research, technical skills, and client engagement has truly set him apart. We're excited to see what he accomplishes next.

Student Signature: Rishabh Sachdeva Date: 30/06/2023

Industry Supervisor Signature: Deepak Budhiraja Date: 30/06/2023

5.1 Appendix H – Monthly Internship Activity Report – Month 2

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Rishabh Sachdeva Student number: x21213909

Company: Waystone Compliance Solutions Month Commencing: June 2023

The second month was dedicated to the comprehensive development of this control framework. Each control was meticulously mapped with strategies for achievement, and alternative implementation methods were analyzed for effectiveness and efficiency. Also, the scoring methodology for the assessment was finalized during this month, Beyond the primary project, my role expanded to assist the team in various other capacities. I was actively involved in developing multiple proposals for government cybersecurity tenders, a task that required a deep understanding of both technical and regulatory requirements. Furthermore, I took the initiative to create various client decks, which served as essential communication tools for our client engagements. I also contributed to the marketing efforts by developing service brochures for Waystone Compliance Solutions. For two of our government entities clients, I created Ransomware Table top exercise focusing on Containment, Eradication and Recovery stages. These brochures effectively encapsulated our service offerings and have been instrumental in client acquisition. Overall, the second month was a blend of in-depth framework development, proposal writing, and client engagement.

Employer comments

Rishabh has done an excellent job again this month. He's made great progress on the DORA framework, paying attention to every detail. He's also been a big help with other important tasks, like helping us with the proposals and creating client materials. We're really pleased with his work.

Student Signature: Rishabh Sachdeva Date: 31/07/2023

Industry Supervisor Signature: Deepak Budhiraja Date: 31/07/2023

5.1 Appendix H – Monthly Internship Activity Report – Month 3

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Rishabh Sachdeva Student number: x21213909

Company: Waystone Compliance Solutions Month Commencing: June 2023

During the third month, the focus was on wrapping up the DORA Pre-Readiness Compliance Assessment Framework. I developed a specialized Assessment Template using the One Trust Platform, which streamlined the evaluation process. To enhance data interpretation, I created Power BI dashboards that offered valuable visualizations and insights. The framework was then subjected to a thorough evaluation by my colleagues to ensure its robustness and practicality. Alongside this, I took on the task of formatting Excel templates that are crucial for data collection and subsequent analysis. I also dedicated time to report writing, where I consolidated our findings and methodologies into a comprehensive document. The month concluded with the finalization of a configuration manual and the creation of essential artifacts. Overall, the third month was a blend of final touches, data visualization, and meticulous documentation, marking a significant phase in my internship.

Employer comments

Rishabh successfully finalized the DORA framework, showcasing his ability to see a complex project through to completion. The Assessment Template he developed on One Trust Platform and the Power BI dashboards he created have added significant value to our operations. We will be using his work to create a service offering for our clients in relation to DORA readiness assessments.

Student Signature: Rishabh Sachdeva Date: 28/08/2023

Industry Supervisor Signature: Deepak Budhiraja Date: 28/08/2023