

Secure Software Design and Engineering Lab Manual



**Jazia.sajid Lab Engineer FCSE
Ghulam Ishaq Khan Institute of Engineering and Technology, Pakistan**

Lab 2 - Risk Management with IriusRisk

Objectives:

- Perform risk identification, assessment, and mitigation using IriusRisk.
 - Create a risk matrix and prioritize risks based on likelihood and impact.
 - Compare the OCTAVE framework with other risk management approaches.
 - Apply NIST standards to enhance risk management strategies.
-

Introduction:

In this lab, students will use IriusRisk to conduct risk management and threat modeling. They will identify risks in software systems, assess their severity, and propose mitigation strategies. Additionally, students will compare different risk management frameworks and explore how NIST standards can enhance risk management processes.

Introduction

Risk management is a critical component of any project, ensuring that potential threats to success are identified, assessed, and mitigated effectively. In the context of the Passport Automation System, risk management helps minimize disruptions, enhances security, and ensures compliance with regulatory standards. This document provides a structured approach to handling risks throughout the project lifecycle.

Risk Management Plan

The risk management plan defines how risks will be handled from identification to mitigation. It outlines the methodology for tracking, analyzing, and responding to risks.

- **Approach:** A proactive strategy will be used to identify risks early and address them before they become major issues.
- **Roles and Responsibilities:**
 - **Project Manager:** Oversees risk management activities, ensures mitigation plans are implemented.
 - **Security Team:** Evaluates cybersecurity risks and compliance.
 - **Development Team:** Identifies technical risks and ensures secure coding practices.

- **Quality Assurance (QA) Team:** Detects issues during testing phases.
- **Stakeholders:** Review risk reports and provide necessary resources.

Risk Identification

Risks related to the **Passport Automation System** can arise from various sources:

1. Technical Risks:

- System downtime or crashes.
- Security vulnerabilities (e.g., unauthorized access, data breaches).
- Integration failures with external databases (e.g., immigration, law enforcement).
- Software bugs affecting application performance.

2. Organizational Risks:

- Delays due to lack of coordination among government agencies.
- Resistance to adopting new technologies.
- Insufficient training for employees using the system.

3. External Risks:

- Cyberattacks targeting sensitive personal data.
- Changes in government regulations affecting compliance.
- Natural disasters affecting data centers or infrastructure.

Risk Assessment

To assess risks, a **Risk Matrix** will be created based on **likelihood (Low, Medium, High)** and **impact (Low, Medium, High)**. The highest priority risks will be addressed first.

- Example Risk Matrix:

Risk	Likelihood	Impact	Risk Level
Unauthorized Data Access	High	High	Critical
System Downtime	Medium	High	High

Risk	Likelihood	Impact	Risk Level
Regulatory Changes	High	Medium	High
Integration Failure	Medium	Medium	Medium

Risk Mitigation Strategies

For each identified risk, a mitigation plan will be developed, including preventive and corrective actions:

1. Unauthorized Data Access:

- Implement multi-factor authentication (MFA).
- Encrypt sensitive data in transit and at rest.
- Regular security audits and vulnerability assessments.

2. System Downtime:

- Deploy redundant servers and failover mechanisms.
- Regular system maintenance and monitoring.

3. Regulatory Changes:

- Continuous compliance monitoring.
- Keep updated with new legal requirements.

4. Integration Failure:

- Conduct interoperability testing before deployment.
- Establish fallback procedures if external databases are unavailable.

Risk Monitoring and Control

Monitoring ensures risks are tracked and mitigated effectively:

- Regular risk assessment meetings.
- Real-time monitoring of security threats.
- Automated alerts for system failures.
- Risk tracking tools (e.g., dashboards, reports).

Risk Communication

Effective communication ensures transparency in risk handling:

- **Stakeholder Reports:** Periodic updates on risk status.
- **Incident Reporting:** A structured process for reporting unexpected risks.
- **Team Meetings:** Weekly risk reviews with all relevant departments.

Contingency Planning

For risks that cannot be fully mitigated, contingency plans will be put in place:

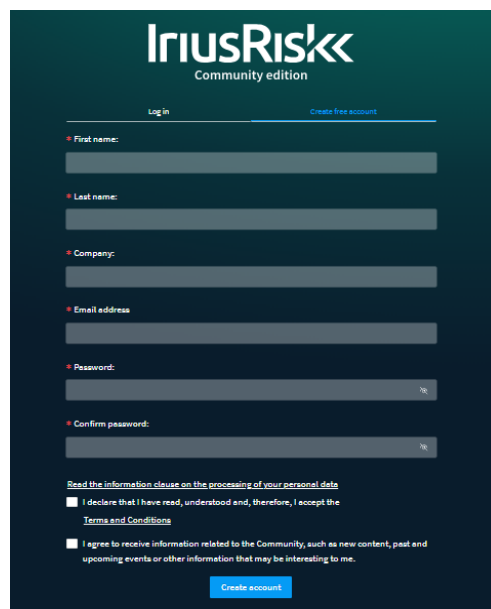
- **Cyberattack Response Plan:** Incident response team activation, forensic analysis, and public communication strategy.
- **System Failure Recovery:** Backup systems, disaster recovery sites.
- **Regulatory Changes**

Steps for Risk Management and Threat Modeling in IriusRisk

Tool walk through

Step 1: Log in to IriusRisk (using community edition)

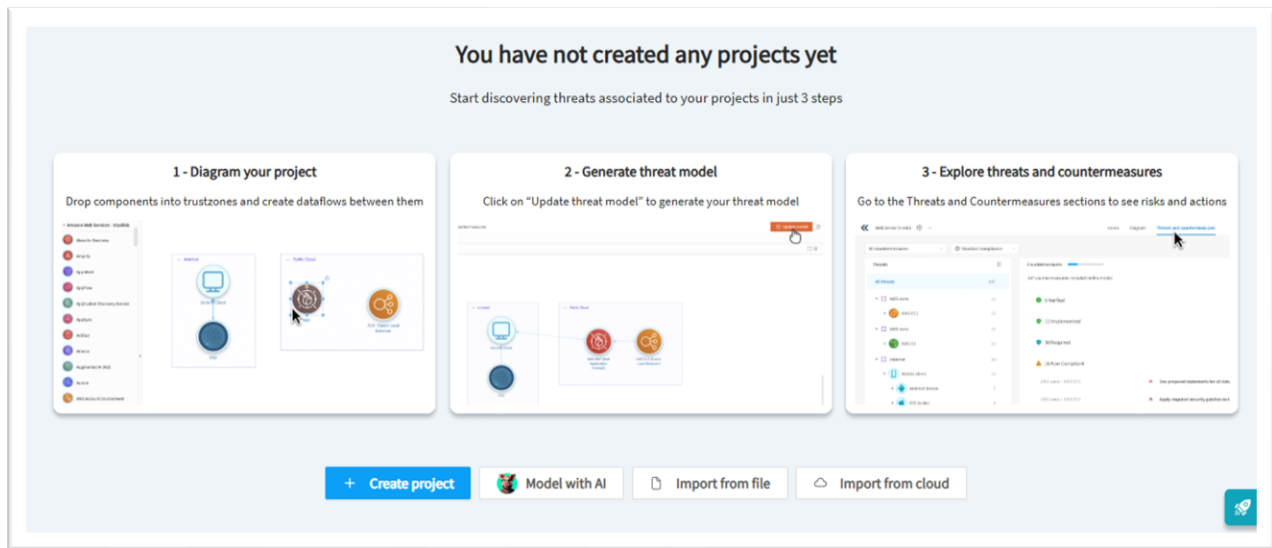
1. Open a web browser and navigate to [IriusRisk login page].
2. Enter your credentials and log in



The screenshot shows the IriusRisk Community edition login page. At the top, the IriusRisk logo is displayed with the text 'Community edition' below it. There are two links: 'Log in' and 'Create free account'. The login form includes fields for 'First name', 'Last name', 'Company', 'Email address', 'Password', and 'Confirm password'. Below the form, there is a link to 'Read the information clause on the processing of your personal data'. Two checkboxes are present: one for 'I declare that I have read, understood and, therefore, I accept the Terms and Conditions' and another for 'I agree to receive information related to the Community, such as new content, past and upcoming events or other information that may be interesting to me.' A 'Create account' button is at the bottom.

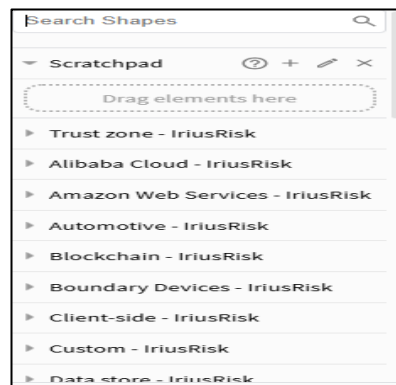
Step 2: Create a New Project

1. Click on **Create New Project**.
2. Enter the project name (e.g., "E-commerce Application Security Model").
3. Provide a brief description.
4. Select the appropriate risk model template.
5. Click **Create**.



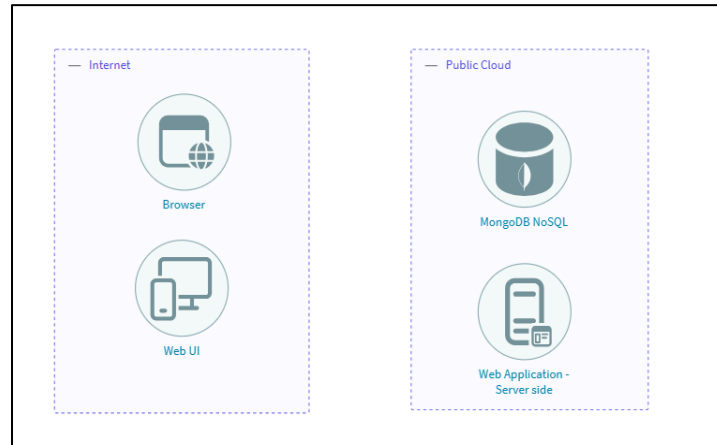
Step 3: Define the Architecture

1. Navigate to the **Architecture** tab.
2. Use the drag-and-drop interface to add components such as:
 - Web Server
 - Database
 - API Gateway
 - Authentication Module
3. Connect the components to reflect data flow.

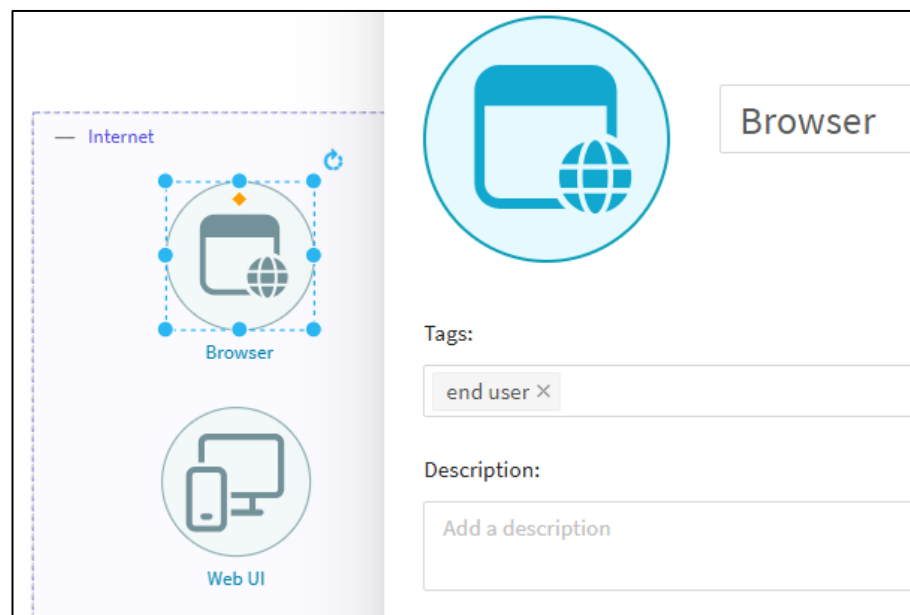


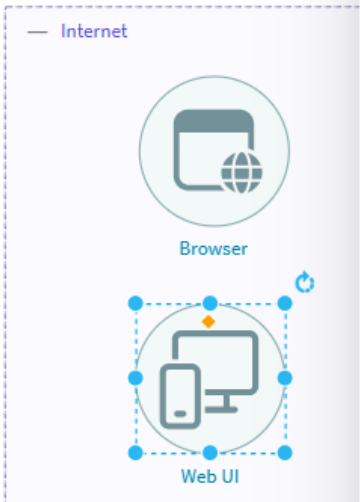
Identify Data Components

- Understand what data the application processes and stores.
- Identify sensitive data such as user credentials, personal information, payment details, or API keys.
- Determine the data flow between different parts of the system.



- Recognize the key data elements in the system and write them in tags.
- Example: **User Credentials, Transaction Data, Logs**, end user etc.






Internet

Browser

Web UI



Web UI


Tags:

Registration × login ×

Description:

Simple authentication method for better understanding of flow.

Questionnaire



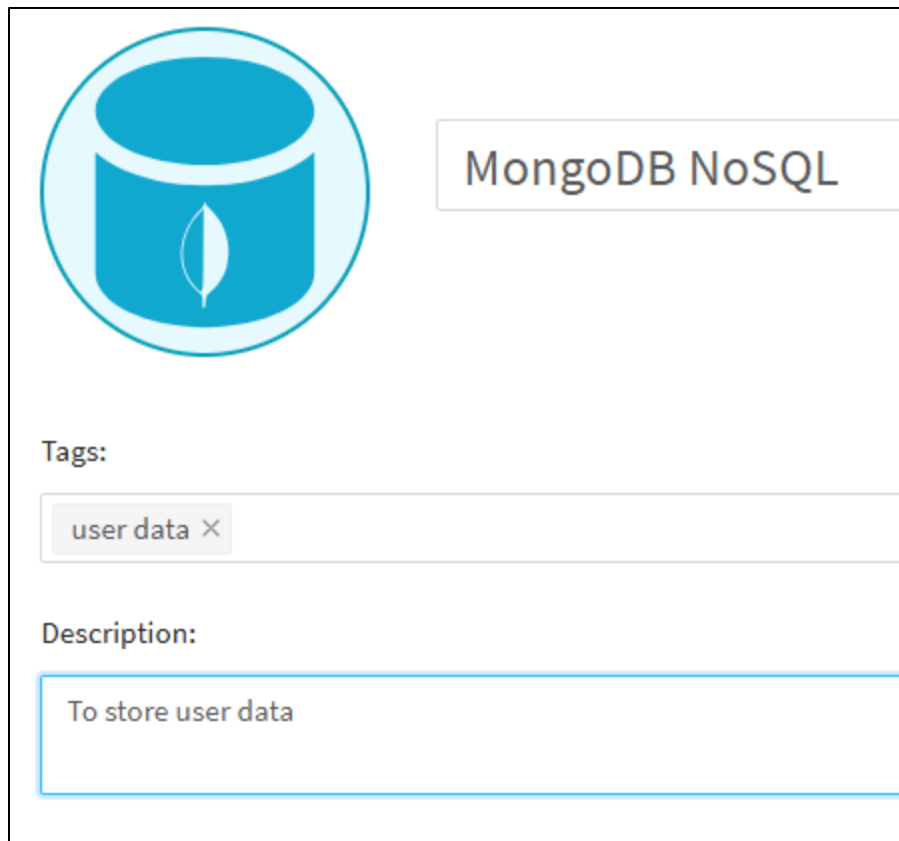
Web Application - Server side

Tags:

expressjs × |

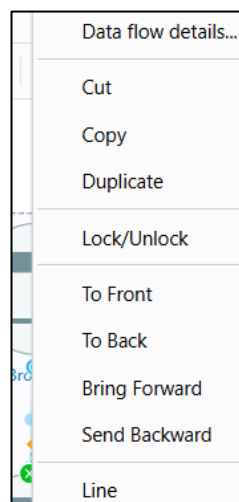
expressjs

Add a description



Determine How Each Component Interacts with Entities

- Identify key system components (e.g., web applications, databases, APIs, external services).
- Analyze how data moves between these components.
- Map out relationships between the entities (e.g., user to web app, web app to database).



- Establish relationships between components and external/internal entities.
- Example:
 - **Web UI → Web Application** (User submits login credentials)
 - **Web Application → MongoDB** (Application stores user data)

Define Use Cases

- Outline the key functions of the application (e.g., user authentication, data retrieval, payment processing).
- Describe typical interactions a user or external system would have with the application.
- Identify different roles (e.g., admin, regular user, external service) and how they interact with the system.

Browser -> Web UI

Source:	Browser
Target:	Web UI
Tags :	<div>Registration × 6 login ×</div>
Assets ⓘ :	<div>Customer Data ×</div> <div>Personally Identifiable Information ×</div>

×

Data flow details

Web UI -> Browser

Source:

Web UI

Target:

Browser

Tags:

response ×

Assets ⓘ :

Select assets

Web UI -> Web Application - Server side

Source:

Web UI

Target:

Web Application - Server side

Tags:

Registration ×

6 login ×

▼

Assets ⓘ :

Customer Data ×

Personally Identifiable Information ×

▼

Identify core functionalities of the application.

Example:

- **Login Process** (User enters credentials → Verified by Web Application → Access granted)
- **Data Retrieval** (User requests data → API fetches data → Data displayed)

Web Application - Server side -> MongoDB NoSQL

Source: Web Application - Server side

Target: MongoDB NoSQL

Tags: user data × Query ×

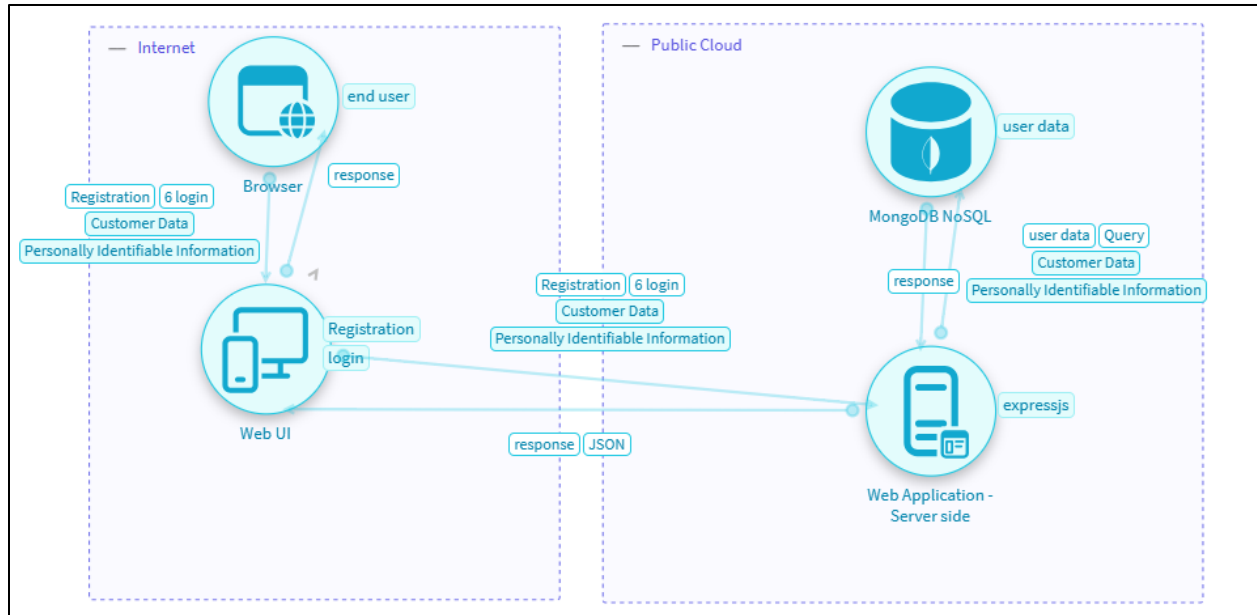
Assets ⓘ : Customer Data × Personally Identifiable Information ×

Identify Entry Points

- Determine how users and other systems interact with the application (e.g., login page, API endpoints, web UI).
- Recognize authentication mechanisms and access control points.
- Determine possible access points where data enters the system.

Example:

- **Web UI (Login Page, API Endpoints, Form Submissions)**
- **External API Integrations**



Determine Assets (Data That Needs Protection)

- Classify critical assets, such as databases, encryption keys, and API endpoints.
- Assess which data is most valuable and at risk of exposure.
- Understand how security policies should be applied to protect these assets.

FILL THE QUESTIONNAIRE

The screenshot shows a 'Web UI questionnaire' form. The 'Assets' section is active, displaying a question about credit card data handling.

Credit Card Data: How is it handled by this component?
Card holder data including the full PAN and CVV number.

Options:

- ☐ Stored
- ☒ Processed
- ☐ Sent from component
- ☐ Received by component

- If the component **stores** credit card data, check "**Stored**" (not recommended due to PCI DSS compliance).
- If the component **handles transactions**, check "**Processed.**"
- If it **sends card data** to another system (e.g., payment gateway), check "**Sent from component.**"
- If it **receives card data**, check "**Received by component.**"
- **Stored** → If the component saves credit card data in a database or file storage.

- **Processed** → If the component handles transactions, encrypts, or validates the card data.
- **Sent from component** → If the component transmits card data to another system or service.
- **Received by component** → If the component receives card data from another system or user input.

Step 4: Identify Threats

1. Click on **Threats**.
2. IriusRisk will auto-generate threats based on STRIDE categories:
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Elevation of Privileges
3. Review the identified threats and modify them if necessary.

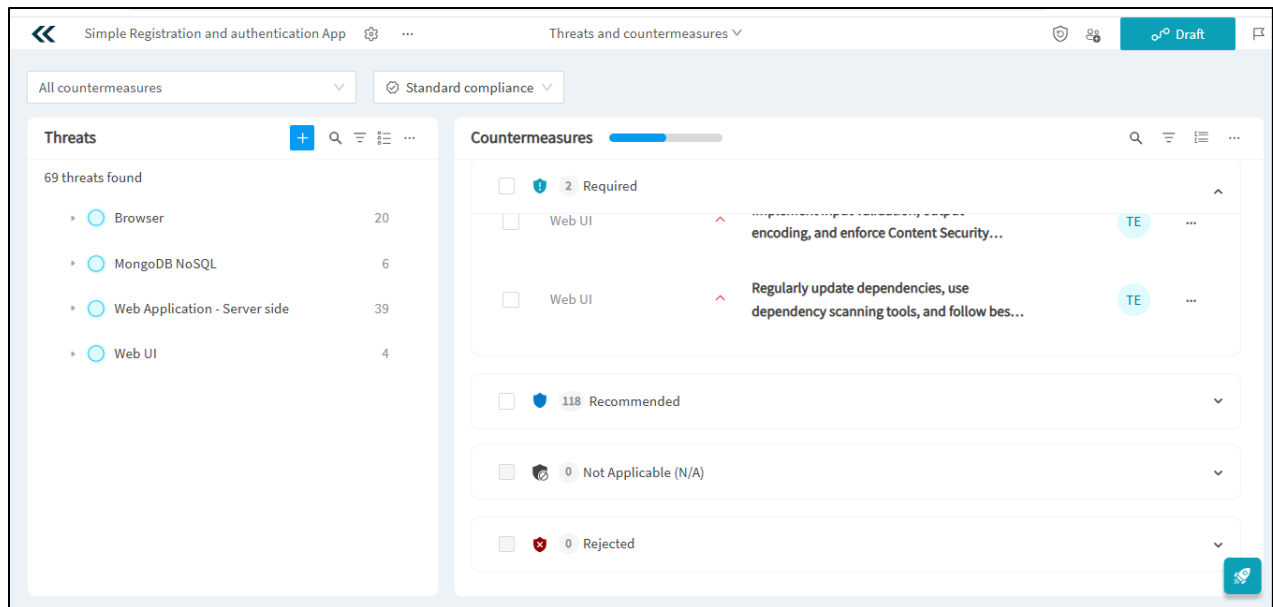
1. Identify Risks Automatically:

- IriusRisk will generate a list of risks based on the system components.
- Review and refine identified risks.

2. Manually Add Additional Risks:

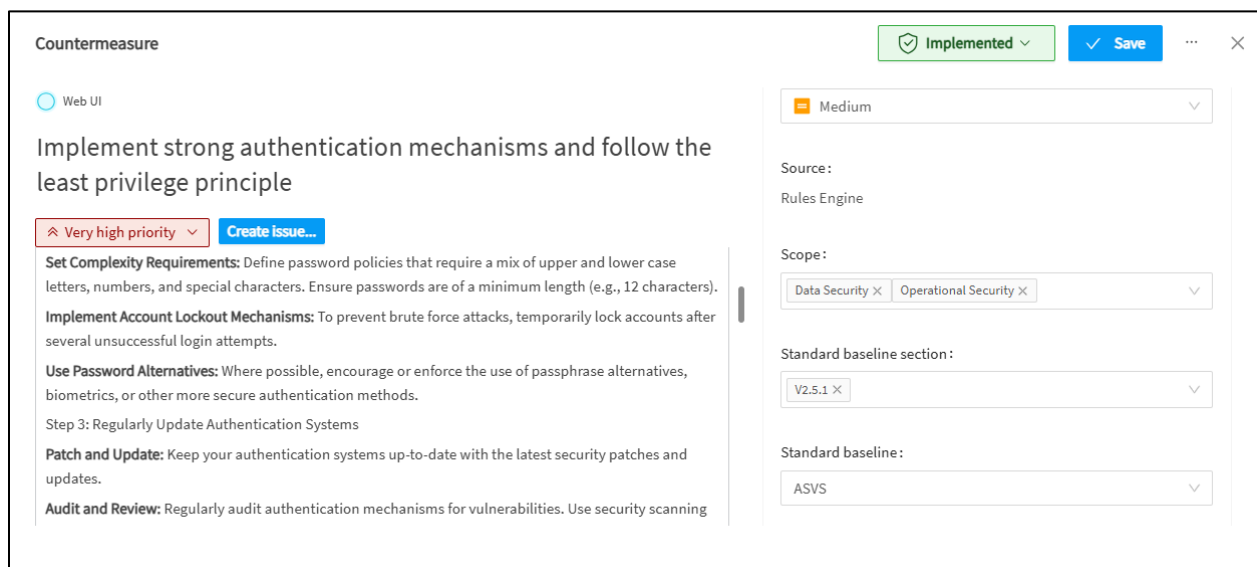
- If needed, manually define additional risks not identified by automation.

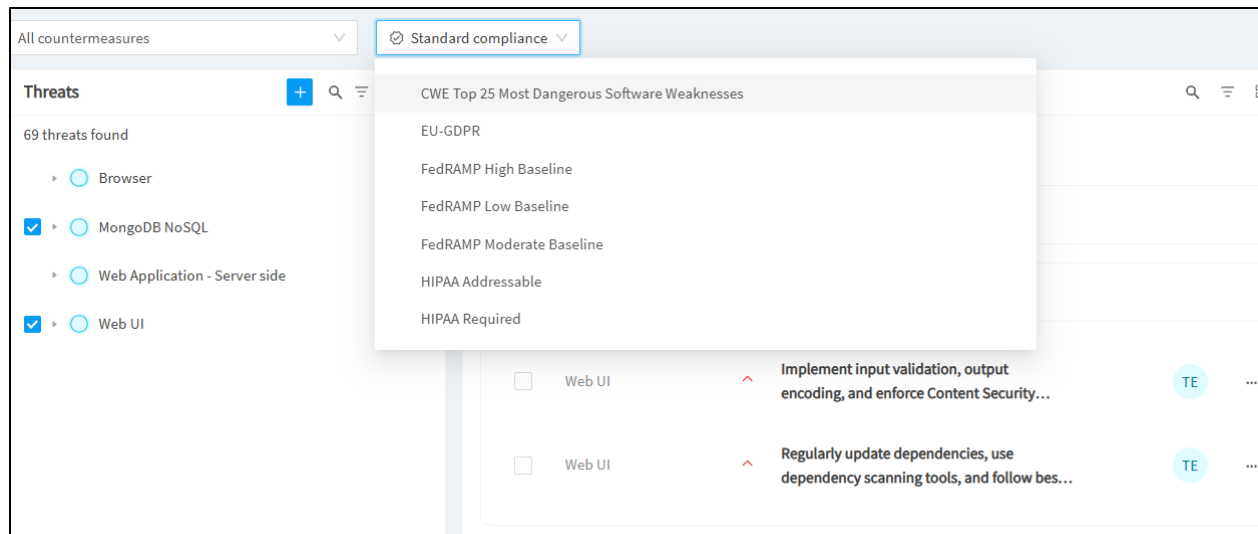
In IriusRisk, risk assessment begins with viewing the **Risk Matrix**, where risks are categorized based on severity. Likelihood and impact values are assigned to each risk, allowing the system to calculate overall risk levels. High-risk threats are prioritized for immediate mitigation. Once risks are identified, mitigation planning involves reviewing **Suggested Controls** provided by IriusRisk, assigning mitigation actions to team members with deadlines, and tracking progress by updating mitigation statuses (e.g., Not Started, In Progress, Completed). This structured approach ensures effective risk management and security enhancement.



Step 6: Define Countermeasures

1. Click on **Countermeasures**.
2. Review the suggested security controls.
3. Assign countermeasures to responsible teams.
4. Mark countermeasures as "Planned" or "Implemented."





Step 7: Generate Reports

1. Navigate to the **Reports** tab.
2. Select the desired report format (e.g., PDF, Excel).
3. Click **Generate Report** and download the document.

Lab ACTIVITY:

Comparison of OCTAVE Framework with Other Approaches

In risk assessment, **octave** stands for "Operationally Critical Threat, Asset, and Vulnerability Evaluation." It's a method used to evaluate and manage risks in a system. In simple terms, **OCTAVE** helps identify what could go wrong in a system, how bad it would be, and how to prevent or reduce those risks.

1. **Identify assets** – What's important in the system (e.g., data, equipment)?
2. **Identify threats** – What could harm those important things (e.g., hackers, natural disasters)?
3. **Assess vulnerabilities** – Where is the system weak or exposed to threats?
4. **Evaluate the impact and risk** – How likely is it that something will go wrong, and what's the impact if it does?

ACTIVITY :

- **Goal:** Understand the differences between OCTAVE and other risk management frameworks.
- **Key Points:**

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
 - Focuses on both technical and organizational risks.
 - Evaluates risks at a high level and integrates business context.
- **Other Approaches:**
 - Traditional risk assessment methods may focus only on technical risks.
 - Frameworks such as FAIR (Factor Analysis of Information Risk) focus on quantitative risk analysis.

Activity: Compare OCTAVE with other risk management approaches and determine which is best suited for different scenarios.

Applying NIST Standards to Risk Management

- **Goal:** Enhance risk management by integrating NIST guidelines.
- **Steps:**
 1. **Review NIST Cybersecurity Framework (CSF):**
 - Identify: Understand system assets and risks.
 - Protect: Implement security controls.
 - Detect: Develop detection mechanisms.
 - Respond: Create an incident response plan.
 - Recover: Plan for business continuity and disaster recovery.
 2. **Map IriusRisk Controls to NIST SP 800-53:**
 - Ensure security measures align with NIST standards.
 - Validate compliance requirements.

Evaluation Tasks for Students:

Scenario:

You are tasked with performing threat modeling for a simple online shopping application using IriusRisk. The application includes key components such as a user login system, shopping cart, payment gateway integration, and an admin panel.

Questions:

1. **Identify Key Components:**
What are the key components of the online shopping application, and how would you map them out in IriusRisk?
2. **Asset Identification:**
What critical assets need to be protected in the online shopping application? How will you define them in IriusRisk?
3. **Threat Identification:**
Using IriusRisk, identify at least three potential threats to the application. What are the common vulnerabilities associated with these threats?
4. **Risk Assessment:**
Assess the risks of the identified threats using IriusRisk. How would you rate the likelihood and impact of each risk in terms of the CIA Triad (Confidentiality, Integrity, Availability)?
5. **Mitigation Strategies:**
For each identified risk, propose at least two mitigation strategies using IriusRisk. How would you implement these to reduce the overall risk?
6. **Report Generation:**
Generate a report using IriusRisk that summarizes the threats, risks, and mitigation strategies for the online shopping application. How would you present these findings clearly and effectively?

Task 1: Identify Risks in IriusRisk

- **Objective:** Use IriusRisk to identify risks in a sample application.
- **Steps:**
 1. Create a new risk assessment project.
 2. Add system components.
 3. Review automatically generated risks.
 4. Document additional risks manually if needed.

Task 2: Assess and Prioritize Risks

- **Objective:** Use the risk matrix to evaluate identified risks.
- **Steps:**

1. View the risk matrix in IriusRisk.
2. Adjust likelihood and impact levels.
3. Rank risks based on severity.

Task 3: Develop Mitigation Plans

- **Objective:** Create mitigation strategies for high-priority risks.
- **Steps:**
 1. Select high-risk threats.
 2. Assign appropriate security controls.
 3. Document mitigation responsibilities and deadlines.

Task 4:

Based on the two scenarios below, fill out the appropriate risk forms:

1. **Risk Accounting Form:** This form requires you to identify the potential risks in the given scenario, assess their likelihood of occurrence, and evaluate the potential impact on the system or organization.
2. **Risk Information Sheet:** This form asks for a detailed description of each identified risk, including its consequences, affected stakeholders, and suggested mitigation or management strategies.

Scenario 1: Unauthorized Data Access in an Online Banking System

A vulnerability in the authentication system of an online banking platform allows attackers to bypass multi-factor authentication (MFA), granting unauthorized access to user accounts. This could lead to financial fraud, compromised user data, and a loss of customer trust. The risk is critical, with a high probability of occurring in the near term. If not mitigated, this could result in significant financial losses, downtime for remediation efforts, and a damaged reputation for the bank.

Scenario 2: Ransomware Attack on a University Network

A ransomware attack targets a university's network, encrypting critical academic and administrative data and demanding payment for decryption. The attack could severely disrupt university operations, including class schedules, grading systems, and ongoing research. The probability of occurrence is medium, with a near-term risk timeframe. If successful, the attack could cause significant downtime, data loss, and operational challenges, making it essential to have proactive defenses and response plans in place."

E.1 Example 1: Risk Accounting Form

Risk Accounting Form ¹	
Identified by:	Date:
	ID #: <i>CM Tracking #</i>
Statement of Risk (with context):	
Consequence: (Cost , Schedule, Performance, Quality)	Risk Magnitude Rm
Severity: (Critical, Serious, Moderate, Minor)	
Probability of occurrence? (High, Medium , Low, %)	
Timeframe of risk? (Near-term, Far-term)	
Mitigation Strategy:	
Different strategies to mitigate this risk. When it must be mitigated.	
Contingency Action and Trigger:	
Risk Grouping:	<i>Other risks (by ID) that will impact this risk or are impacted by this risk</i>

ID:		Risk Information Sheet²		Identified:	
Priority:		Statement of Risk:			
Probability:					
Impact:					
Timeframe:		Origin:	Class:		Assigned To:
Context:					
Mitigation Strategy:					
Contingency Action and Trigger:					
Status:				Status Date:	
Approval:		Closing Date:		Closing Rationale:	

