ITSU2006R IT PROJECT MANAGEMENT

CYBERSECURITY RISK ASSESSMENT AND MITIGATION STRATEGY IMPLEMENTATION FOR AN E-COMMERCE PLATFORM

SUBMITTED TO:

DR. SAROJ HIRANWAL

SUBMITTED BY:

RHYTHM (LEADER)	60652
AMROJPREET SINGH	60726
VALENTINE KIPLAGAT	64497
KUNAL RELAN	60550

DATE:

25MAY 2025

INTRODUCTION

E-commerce platforms, given they handle myriad customer and financial data that are extremely sensitive, are prime targets for cyberattacks in this digital economy of ours. Being that there's an ever-increasing phase of threats from data breaches to ransomware and phishing, it is crucial to prevent the risk through cybersecurity measures. **This report marks a complete cybersecurity risk analysis and risk mitigation strategy for an e-commerce platform design.** It looks to expose vulnerable areas, determine the effect and likelihood of certain cyber threats, and provide recommendations on the placement of controls to increase the security status of the platform.

This report integrates the risk management framework with security best practices to provide actionable recommendations including prevention, detection, and response to cyber threats. Such an analytical approach promotes data integrity and confidentiality while increasing consumer confidence, and business continuity. Such careful risk analysis and scientifically directed resolution show the need for setting up proactive cybersecurity plans amid the ever-changing nature of online trade.

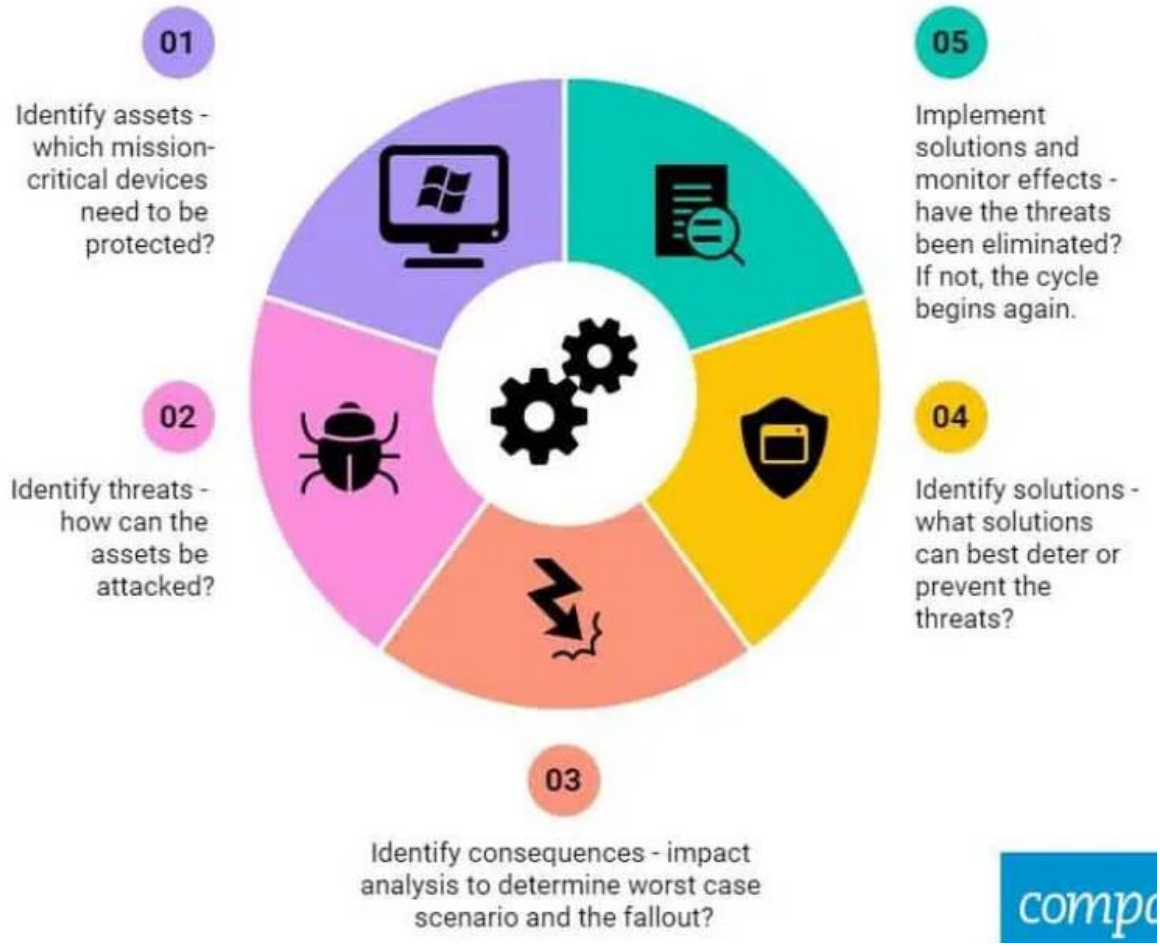


Figure 1 Infographic showing each step of cybersecurity risk management [1]

WORKFLOW ANALYSIS

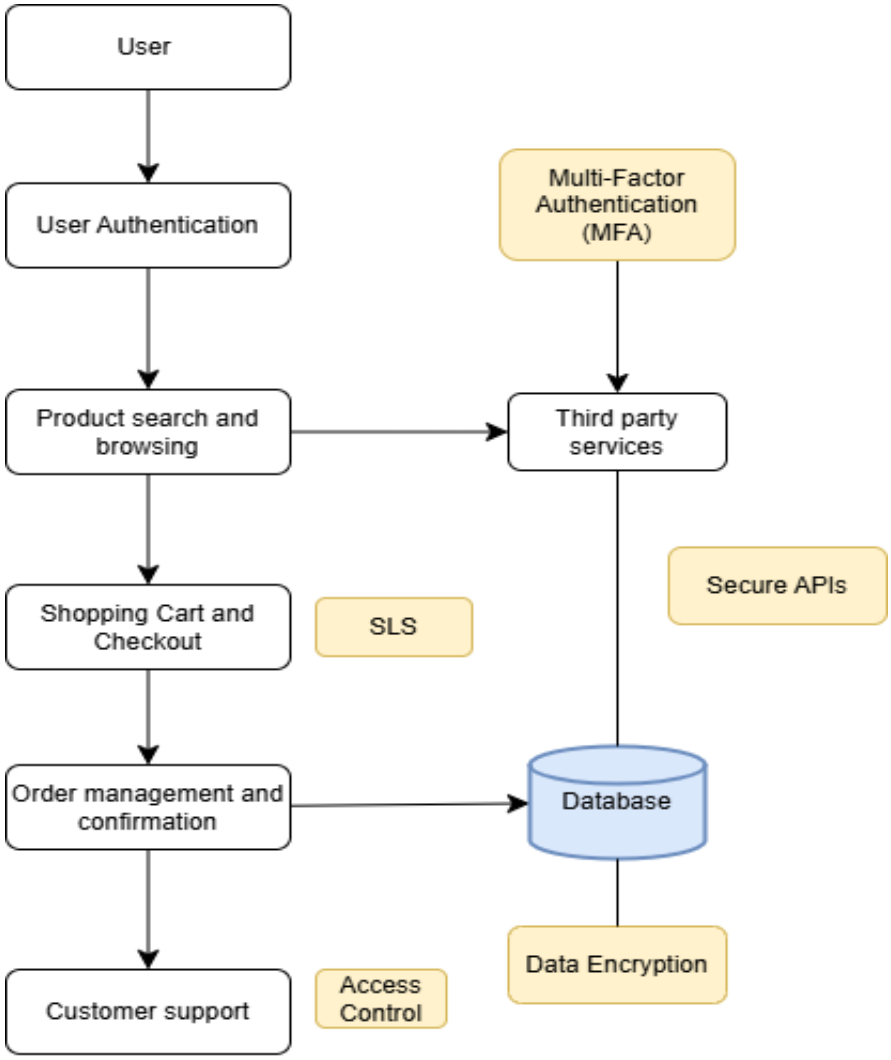
Workflow analysis is the process of analysing a system's task sequence and data flows to find security risk, redundancies, and inefficiencies. In Cybersecurity workflow analysis aims to ensure that each step in the digital process functions properly and adheres to secure practices to protect the system from threats and ensure information confidentiality, integrity and availability.

To help understand the analysis plan, The system should include;

Frontend: This is the user interface which entails product browsing, shopping cart, checkout
Backend: This includes the payment gateway, orders that are being processed and the Database.
Third party Intergrations: These are the payment providers, shipping analytics and CRM

WORKFLOW SEQUENCE

- User Authentication and Authorization
- Product Search and Browsing
- Shopping Cart and Checkout
- Payment Processing
- Order Management and Confirmation.
- Customer Support through Portal.
- Data Storage and Access



Workflow Analysis Diagram

PROJECT CHARTER

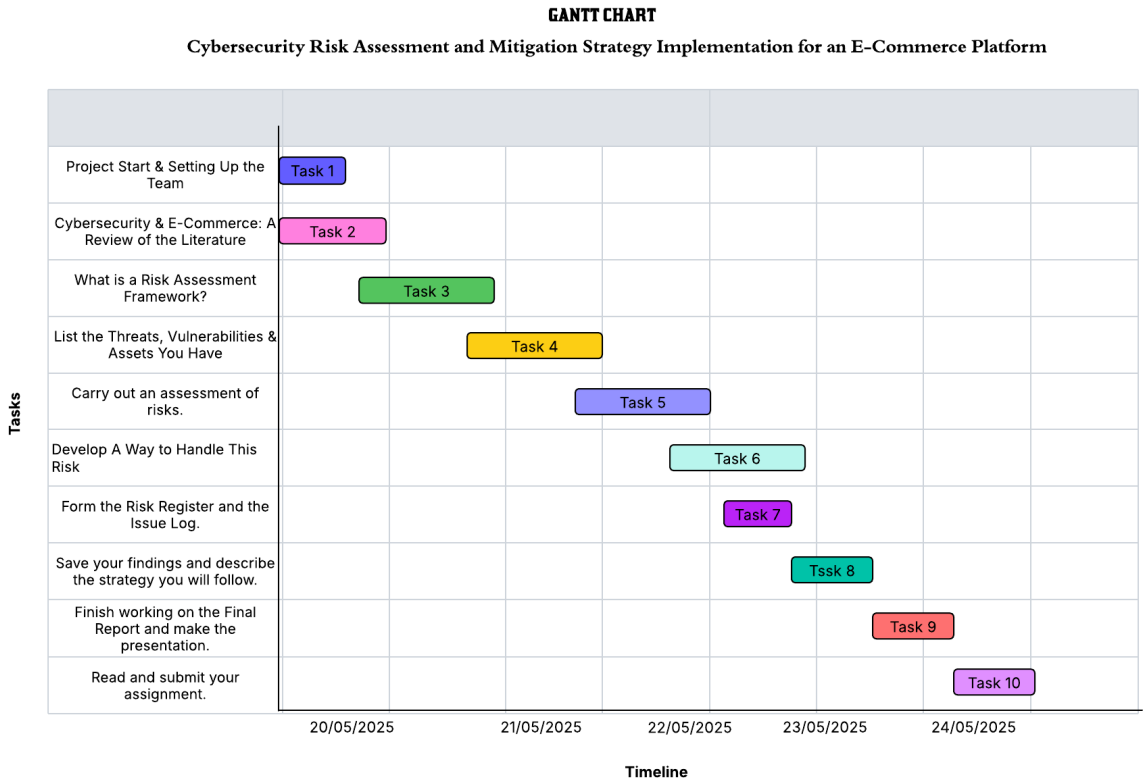
Details	Elements
Project Name	Cybersecurity Risk Assessment and Mitigation Strategy
Project Manager	Rhythm
Project Sponsor	Amroj, Kunal, and Valentine
Start Date	20 May 2025
End Date	24 May 2025
Budget	AUD $50,000
Key Stakeholders	Project Sponsor, Security Analysts, DevOps Team, Quality Assurance Team
Project Description	A project to strengthen cybersecurity posture through vulnerability assessment and the application of modern mitigation techniques tailored for an e-commerce platform
Objectives	• Identifying and prioritizing security risks • Implementing mitigation measures • Ensuring compliance with industry standards
Success Criteria	• Reduction in vulnerabilities by 80% • Zero critical security incidents post-implementation. • No high severity issues remaining

GANTT CHART

TASK TABLE (with timelines, dependencies & responsible person)

Task No.	Task Name	Start Date	End Date	Dependencies	Responsible Person
1	Project Start & Setting Up the Team	20/05/2025	21/05/2025	-	Project Manager
2	Cybersecurity & E-Commerce: A Review of the Literature	21/05/2025	22/05/2025	Task 1	Project Manager
3	What is a Risk Assessment Framework?	22/05/2025	23/05/2025	Task 2	Project Manager
4	List the Threats, Vulnerabilities & Assets You Have	22/05/2025	23/05/2025	Task 3	Project Manager
5	Carry out an assessment of risks.	22/05/2025	23/05/2025	Task 4	Risk Manager
6	Develop A Way to Handle This Risk	22/05/2025	23/05/2025	Task 5	Risk Manager
7	Form the Risk Register and the Issue Log.	22/05/2025	23/05/2025	Task 6	Risk Manager
8	Save your findings and describe the strategy you will follow.	23/05/2025	24/05/2025	Task 6 & 7	Project Manager
9	Finish working on the Final Report and make the presentation.	23/05/2025	24/05/2025	Task 8	Team Lead
10	Read and submit your assignment.	24/05/2025	24/05/2025	Task 9	Team Lead

A Gantt Chart was developed using the timeline given above with the help of Lucid chart tool.



RISK AND ISSUE MANAGEMENT PLAN

RISK IDENTIFICATION AND ASSESSMENT

Risk ID	Description	Likelihood	Impact	Risk Level	Category
R1	Phishing is a common form of attack to get at a customer's login information.	High	High	Critical	Cyber Threat
R2	Distributed Denial of Service is the name given to these attacks.	Medium	High	High	Network Availability
R3	There are security problems with using the APIs for payment gateways.	Low	High	Medium	Application Security
R4	Employees using their access in a wrong way.	Medium	Medium	Medium	Human Factor
R5	Data might be leaked when we are migrating or patching.	Low	Medium	Low	Data Handling
R6	Cases of not following compliance rules (such as GDPR or PCI-DSS).	Medium	High	High	Regulatory

RISK MITIGATION STRATEGIES

Risk ID	Mitigation Strategy	Owner
R1	Introduce MFA and show employees how to identify phishing.	Security Team
R2	Use a Web Application Firewall and get DDoS protection.	Network Admin
R3	Keep conducting scans of your APIs and rely on authorization tokens for authentication.	Development Team
R4	Use RBAC, check what users are doing through logs.	HR & IT Security

R5	Always use security for data as it travels, test out all migration efforts in advance and have an undo plan ready.	Developers
R6	Check your compliance, update your privacy policy and record the way you deal with your data.	Compliance Officer

ISSUE LOG AND TRACKING TABLE

Issue ID	**Issue Description**	**Status**	**Reported On**	**Resolution Action**	**Owner**
I1	Problems with understanding GitHub commit schedules.	Open	21/05/2025	Group meetings began each day of the week.	Team Leader
I2	Failing to retrieve some references is what delays the literature review in research.	Resolved	22/05/2025	Added more members to the support team.	Report Lead
I3	Not all members can see the assignments in Jira.	Resolved	22/05/2025	Updates to who can work on specific sections of the board.	Jira Admin
I4	The responsibilities under mitigation strategy are unclear.	Open	23/05/2025	Setting up a session that simplifies the confusion.	Security Lead

CHANGE MANAGEMENT PLAN

Change request form template

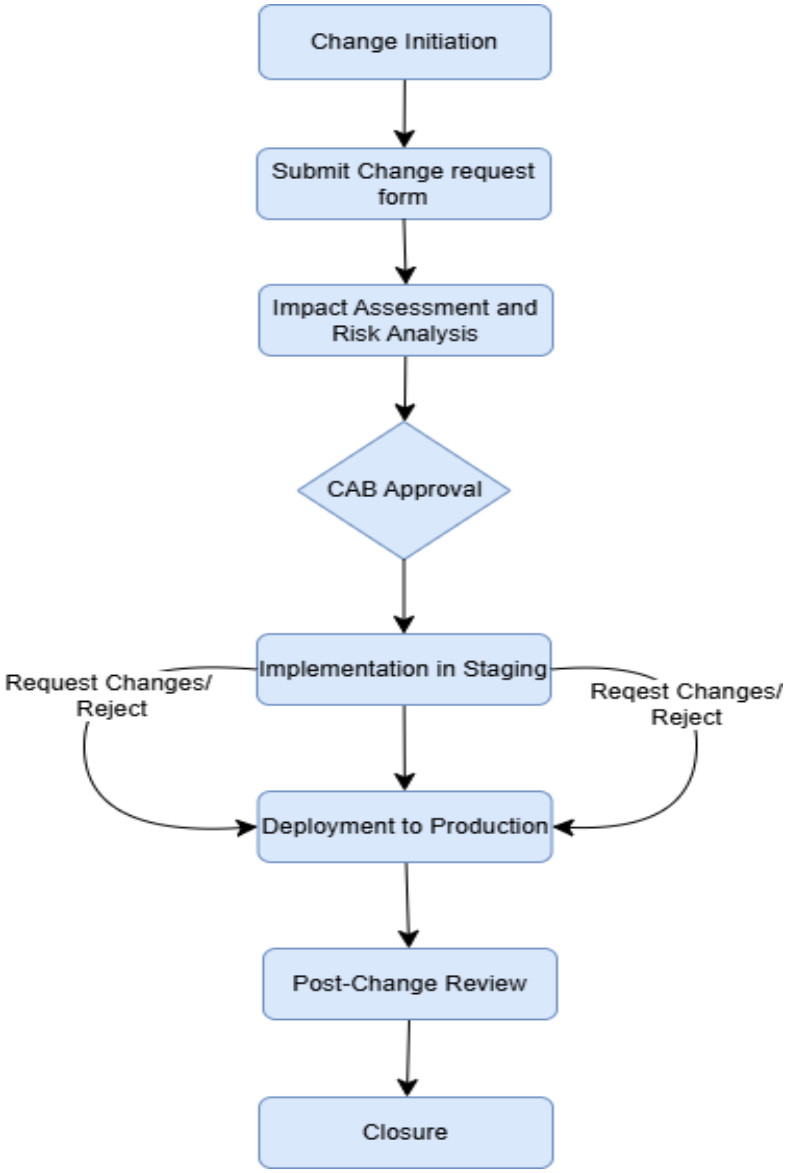
Section	Details
Change request ID	CR-001-025
Date Submitted	[DD/MM/YYYY]
Requester name	[Full Name]
Department	[e.g IT, Cybersecurity]
Change title	[Short summary of the change]
Change description	[Detailed description of the proposed change]
Reason for change	[Why is the change needed]
Affected systems	[e.g authentication system, Payment gateway]
Risk assessment	[Low/Medium/High]
Expected impact	[Impact on users, system, performance]
Rollout plan	[Steps to implement the change]
Rollback plan	[steps to revert change if needed]
Testing requirements	[pre-deployment tests, QA process]
Change classification	[Standard/Normal/Emergency]
Target Implementation date	[DD/MM/YYYY]
Submitted by	[Full Name]
Approval Signatures	[Project Manager, Cybersecurity Lead, QA Lead

Sample of Filled change request form

Section	**Details**
Change request ID	CR-001-025
Date Submitted	20/5/2025
Requester name	Valentine Kiplagat
Department	Cybersecurity, IT
Change title	Enabling MFA for the admin panel
Change description	We would like to curb risks of unauthorized access; therefore, we propose the enabling of MFA on all admin accounts
Reason for change	Following the previous training program MFA was recommended as the best mitigation strategy
Affected systems	Admin login
Risk assessment	Medium
Expected impact	Minimal user friction for admins

Rollout plan	Test each stage before full rollout, Implement via Auth0 API
Rollback plan	Revert to previous auth method and disable new policy via GitHub
Testing requirements	Functional and usability
Change classification	Normal
Target Implementation date	24/5/2025
Submitted by	Valentine Kiplagat
Approval Signatures	To be signed by; Project Manager, Cybersecurity Lead, QA Lead

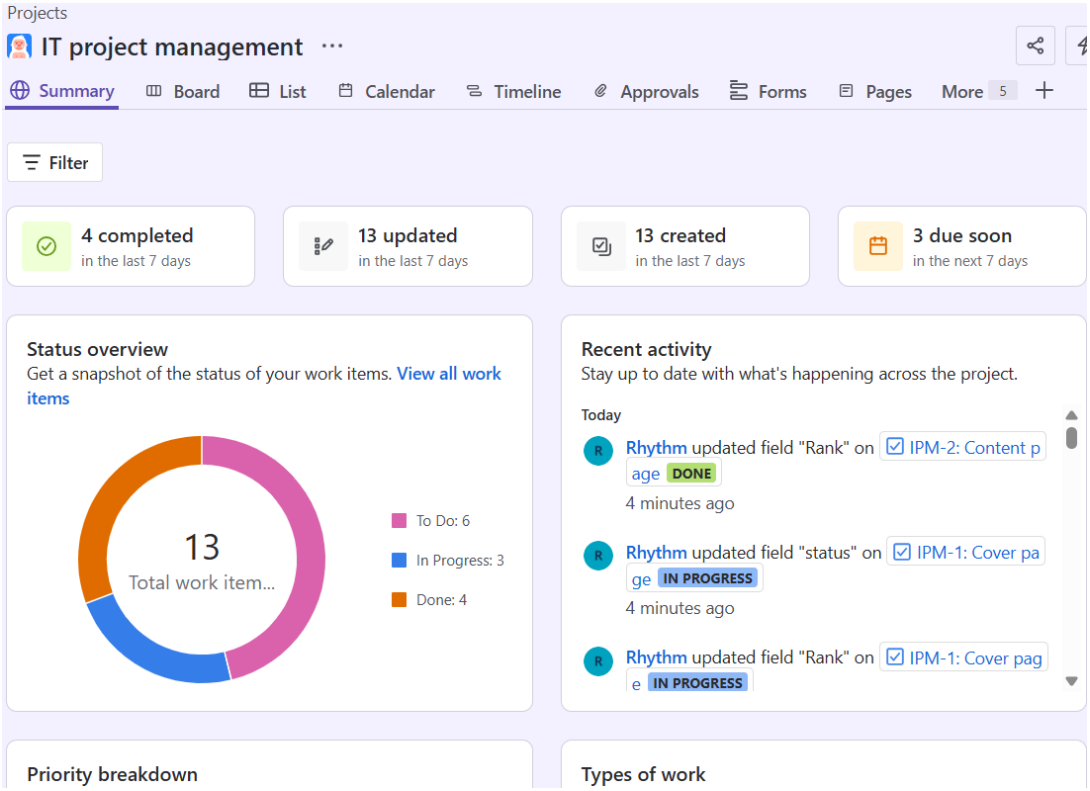
Change Approval Workflow

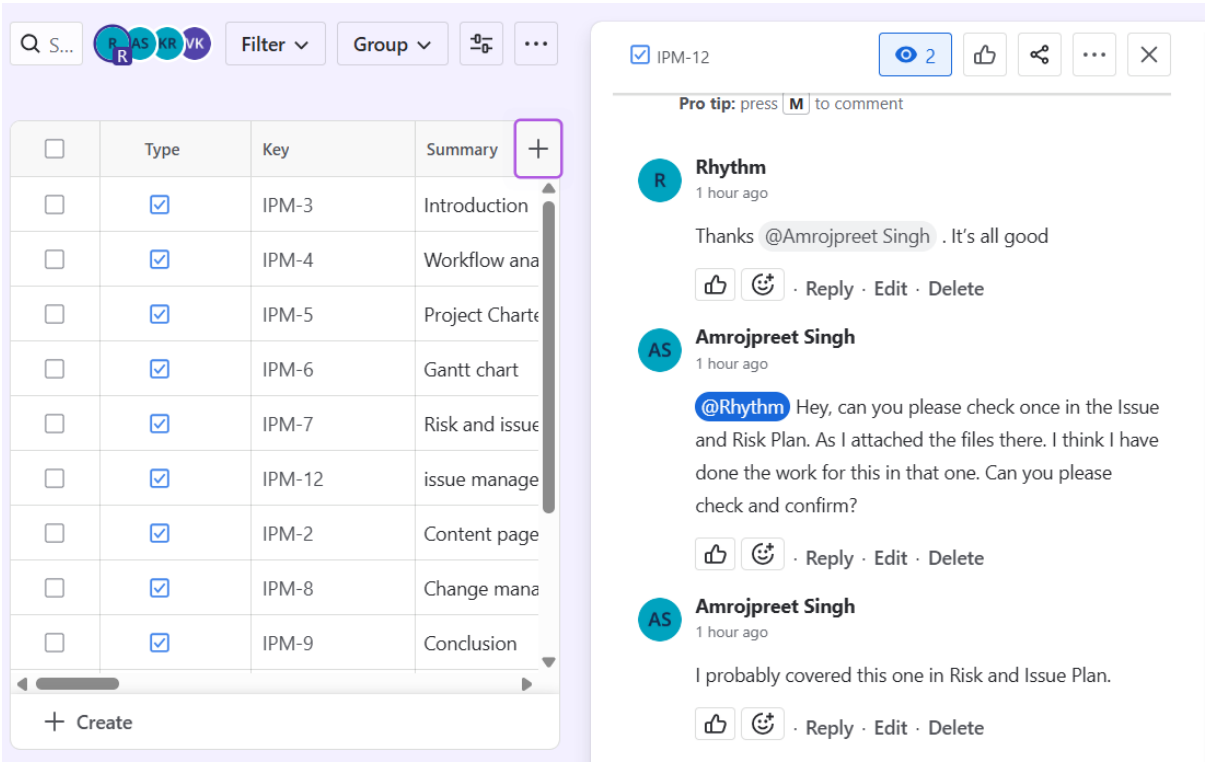


CONCLUSION

This cybersecurity risk assessment and mitigation project is vital in strengthening the e-commerce platform's defenses against modern cyber threats. By systematically identifying vulnerabilities and implementing appropriate security measures, the platform will be better equipped to handle threats, reduce downtime, and protect sensitive user data. By leveraging vulnerability assessments, penetration testing, and GitHub for configuration management, the organization can enhance its security posture while maintaining compliance. The integration of GitHub as a configuration management tool ensures traceability, accountability, and enhanced collaboration throughout the project lifecycle. The use of risk-based prioritization and clear change control processes further guarantees that mitigation strategies are both effective and sustainable.

DISCUSSION USING JIRA/GITHUB





REFERENCES

[1] P. Bischoff, “Cybersecurity Risk Management: What It Is and How to Do It Well,” *Comparitech*, May 7, 2024. [Online]. Available: https://www.comparitech.com/net-admin/cybersecurity-risk-management/

M. Gregory, "Using GitHub for Version Control and Team Collaboration," *IEEE Software*, vol. 35, no. 5, pp. 67–71, Sept.-Oct. 2018.

NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Gaithersburg, MD, USA, Version 1.1, Apr. 2018.

D. Geer, "Security Strategies for E-Commerce Systems," *IEEE Internet Computing*, vol. 6, no. 6, pp. 18–21, Nov.-Dec. 2002

B. Babb, “Workflow Analysis: Key to Building Better Processes,” *Pipefy*, Jul. 16, 2022. https://www.pipefy.com/blog/workflow-analysis/