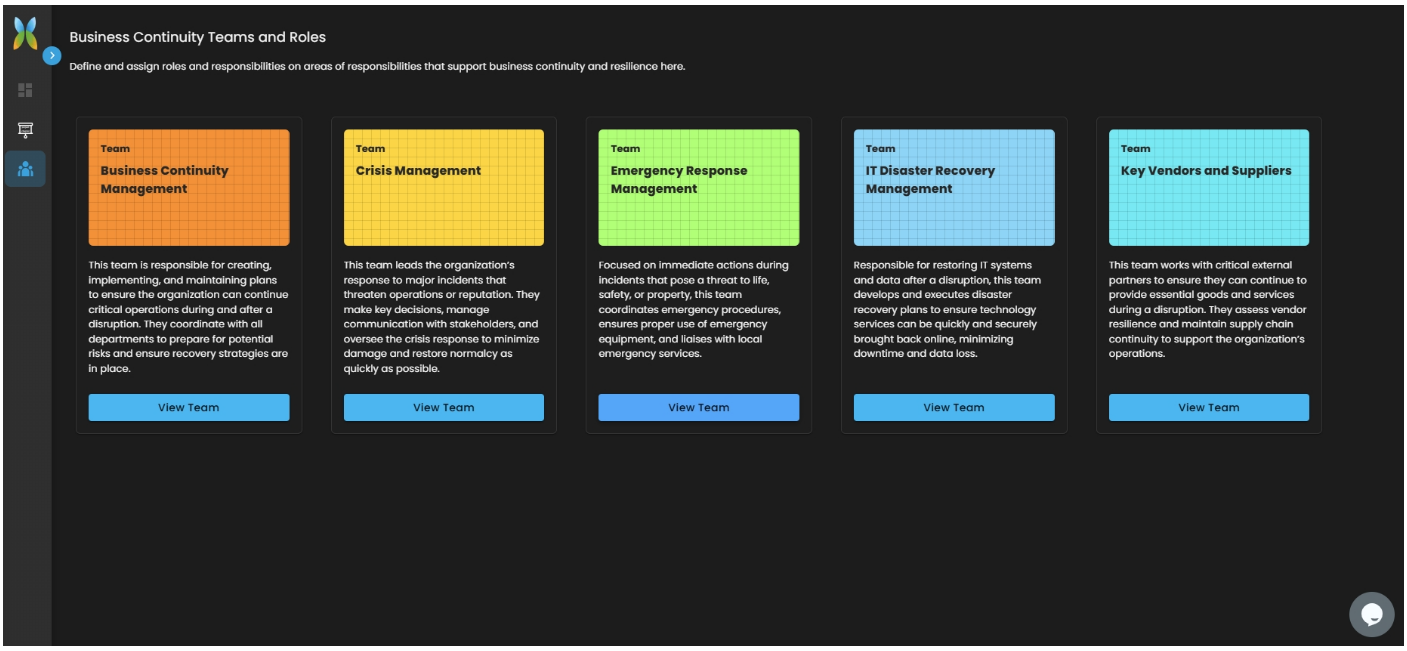
Daily Update: September 13

Here are the main updates of the CISO Workplace:

Business Continuity Management Updates:

BCM Team and Roles Page



Business Continuity Teams and Roles

Define and assign roles and responsibilities on areas of responsibilities that support business continuity and resilience here.

Team
Business Continuity Management

This team is responsible for creating, implementing, and maintaining plans to ensure the organization can continue critical operations during and after a disruption. They coordinate with all departments to prepare for potential risks and ensure recovery strategies are in place.

Team
Crisis Management

This team leads the organization's response to major incidents that threaten operations or reputation. They make key decisions, manage communication with stakeholders, and oversee the crisis response to minimize damage and restore normalcy as quickly as possible.

Team
Emergency Response Management

Focused on immediate actions during incidents that pose a threat to life, safety, or property, this team coordinates emergency procedures, ensures proper use of emergency equipment, and liaises with local emergency services.

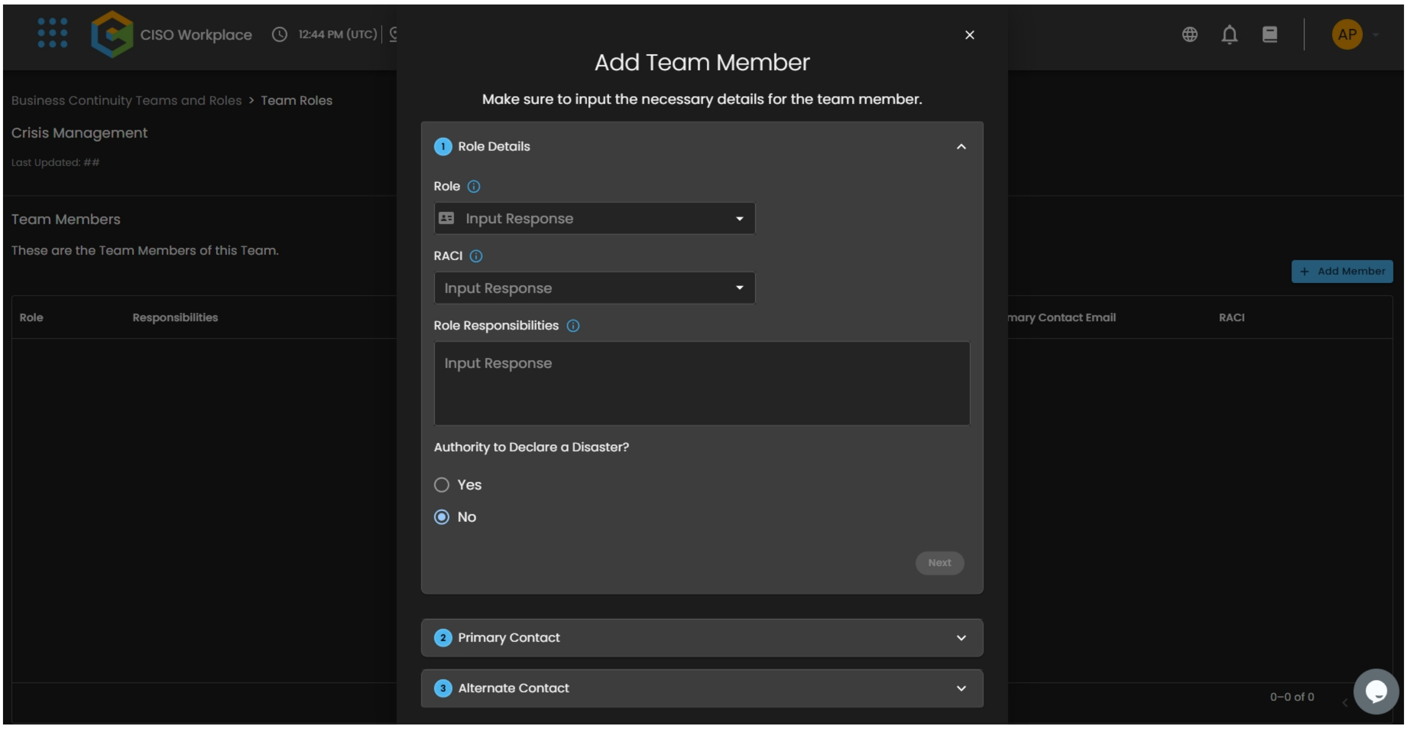
Team
IT Disaster Recovery Management

Responsible for restoring IT systems and data after a disruption, this team develops and executes disaster recovery plans to ensure technology services can be quickly and securely brought back online, minimizing downtime and data loss.

Team
Key Vendors and Suppliers

This team works with critical external partners to ensure they can continue to provide essential goods and services during a disruption. They assess vendor resilience and maintain supply chain continuity to support the organization's operations.

BCM Create Team Role Forms



Business Continuity Teams and Roles > Team Roles

Crisis Management

Last Updated: ##

Team Members

These are the Team Members of this Team.

Role	Responsibilities	...mary Contact Email	RACI

0–0 of 0

Add Team Member

Make sure to input the necessary details for the team member.

1 Role Details

Role: Input Response

RACI: Input Response

Role Responsibilities: Input Response

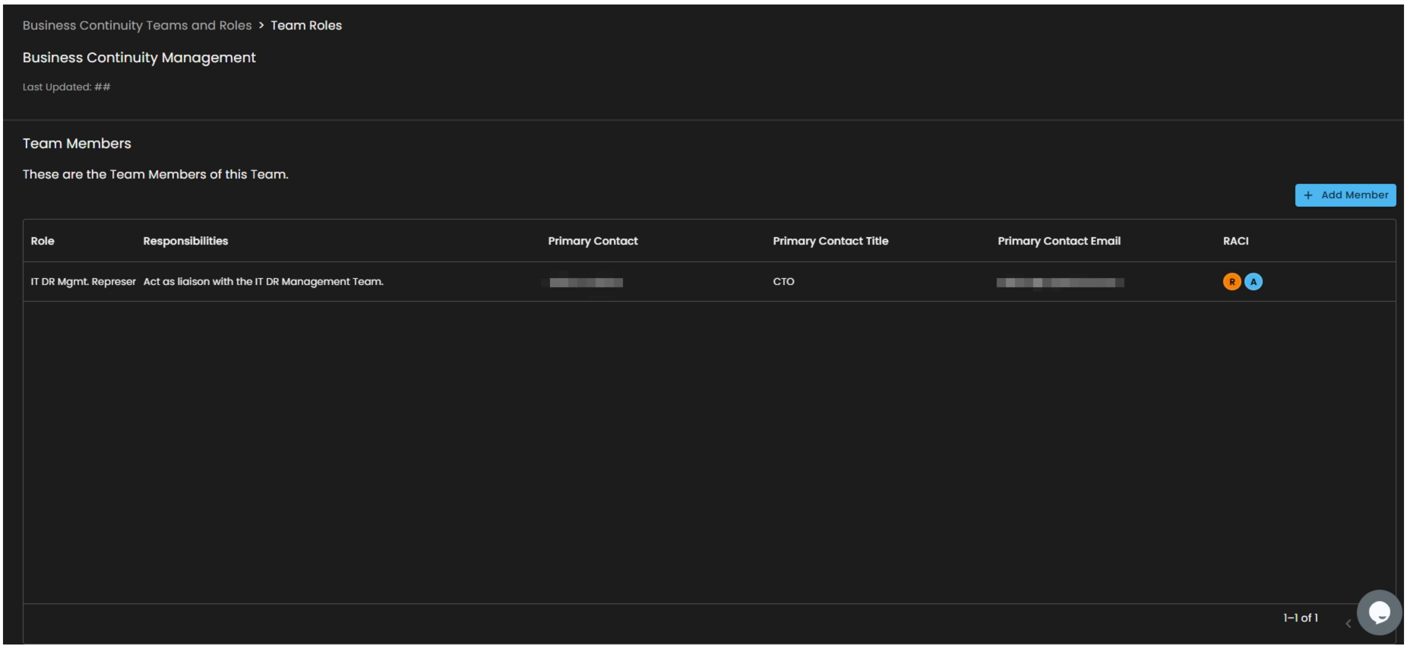
Authority to Declare a Disaster?

○ Yes

● No

2 Primary Contact

3 Alternate Contact



Business Continuity Teams and Roles > Team Roles

Business Continuity Management

Last Updated: ##

Team Members

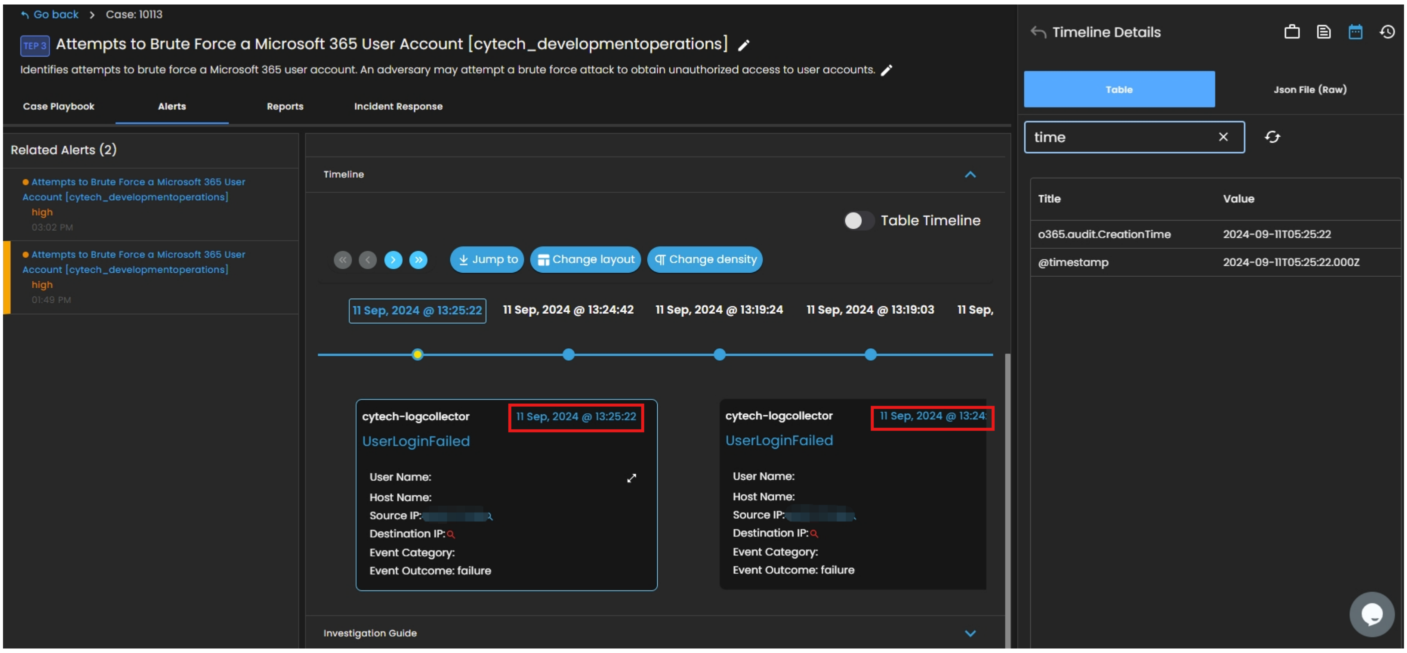
These are the Team Members of this Team.

Role	Responsibilities	Primary Contact	Primary Contact Title	Primary Contact Email	RACI
IT DR Mgmt. Represer	Act as liaison with the IT DR Management Team.	[redacted]	CTO	[redacted]	R A

1–1 of 1

CIM Updates:

Alert Timeline Timestamp Fix in CIM-v3



Go back > Case: 10113

TEP 3 Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Related Alerts (2)

- Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations] high 03:02 PM
- Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations] high 01:49 PM

11 Sep, 2024 @ 13:25:22 | 11 Sep, 2024 @ 13:24:42 | 11 Sep, 2024 @ 13:19:24 | 11 Sep, 2024 @ 13:19:03 | 11 Sep,

cytech-logcollector 11 Sep, 2024 @ 13:25:22
UserLoginFailed
User Name:
Host Name:
Source IP:[redacted]
Destination IP:
Event Category:
Event Outcome: failure

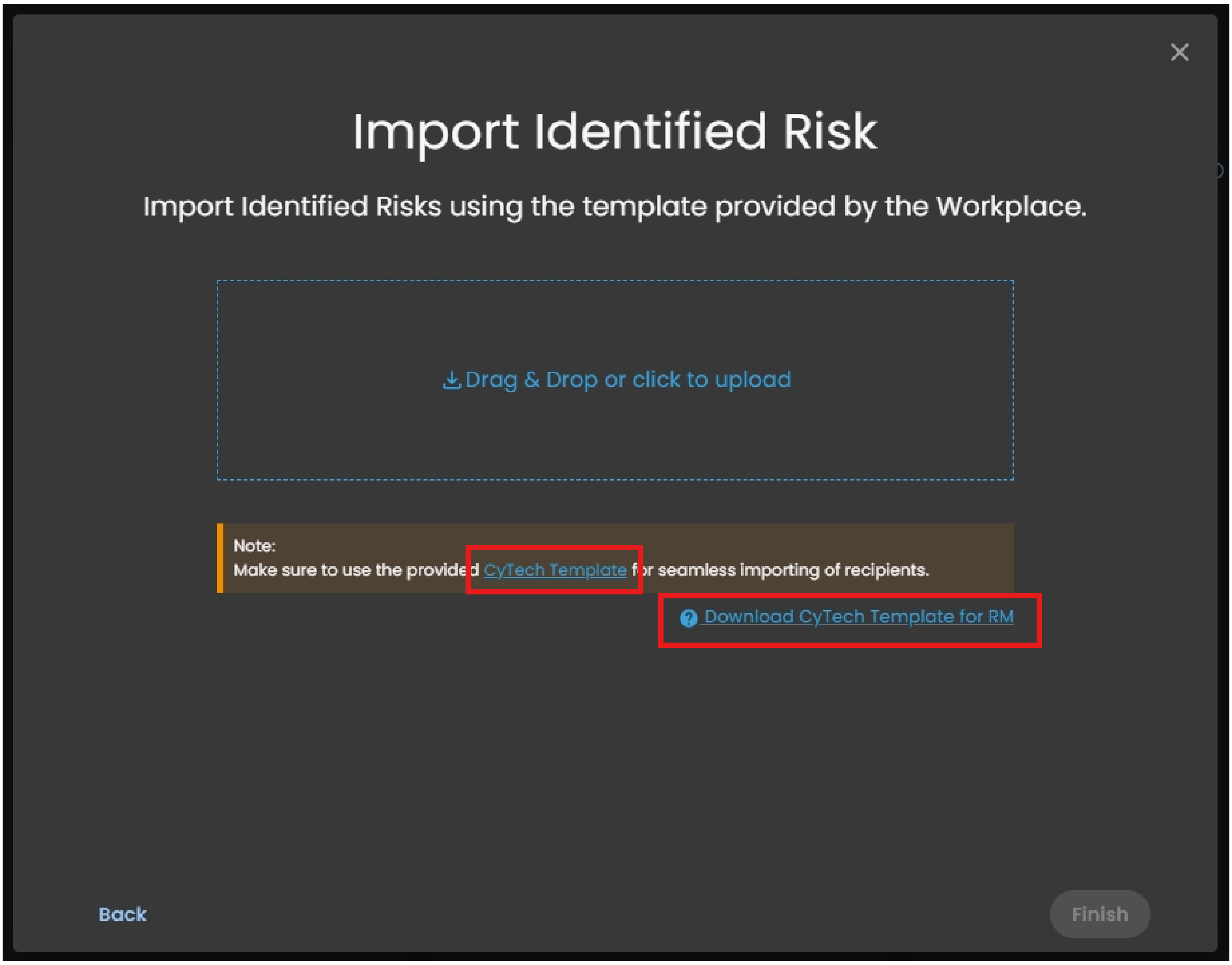
cytech-logcollector 11 Sep, 2024 @ 13:24:
UserLoginFailed
User Name:
Host Name:
Source IP:[redacted]
Destination IP:
Event Category:
Event Outcome: failure

time

Title	Value
o365.audit.CreationTime	2024-09-11T05:25:22
@timestamp	2024-09-11T05:25:22.000Z

RM Updates

Download Excel Template for Risk Importer



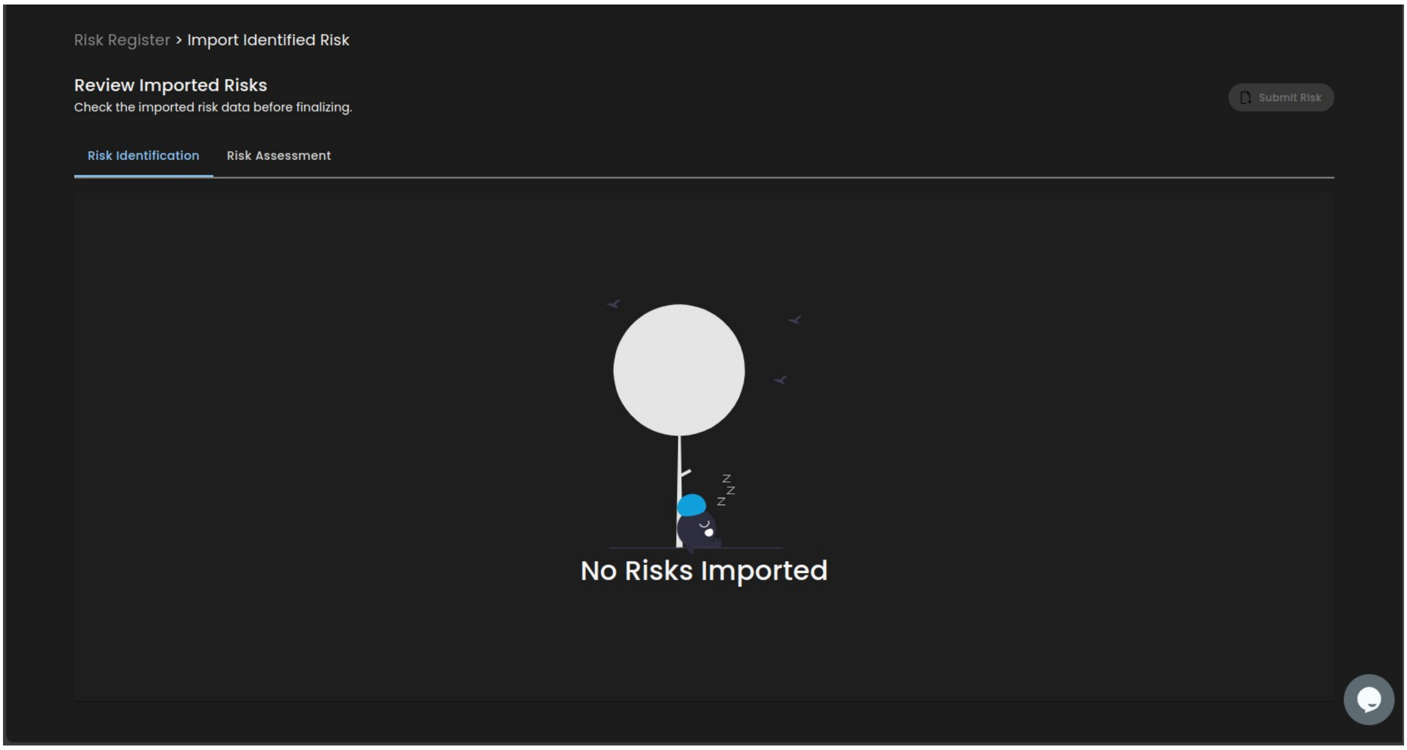
Import Identified Risk

Import Identified Risks using the template provided by the Workplace.

Note:
Make sure to use the provided CyTech Template for seamless importing of recipients.

Download CyTech Template for RM

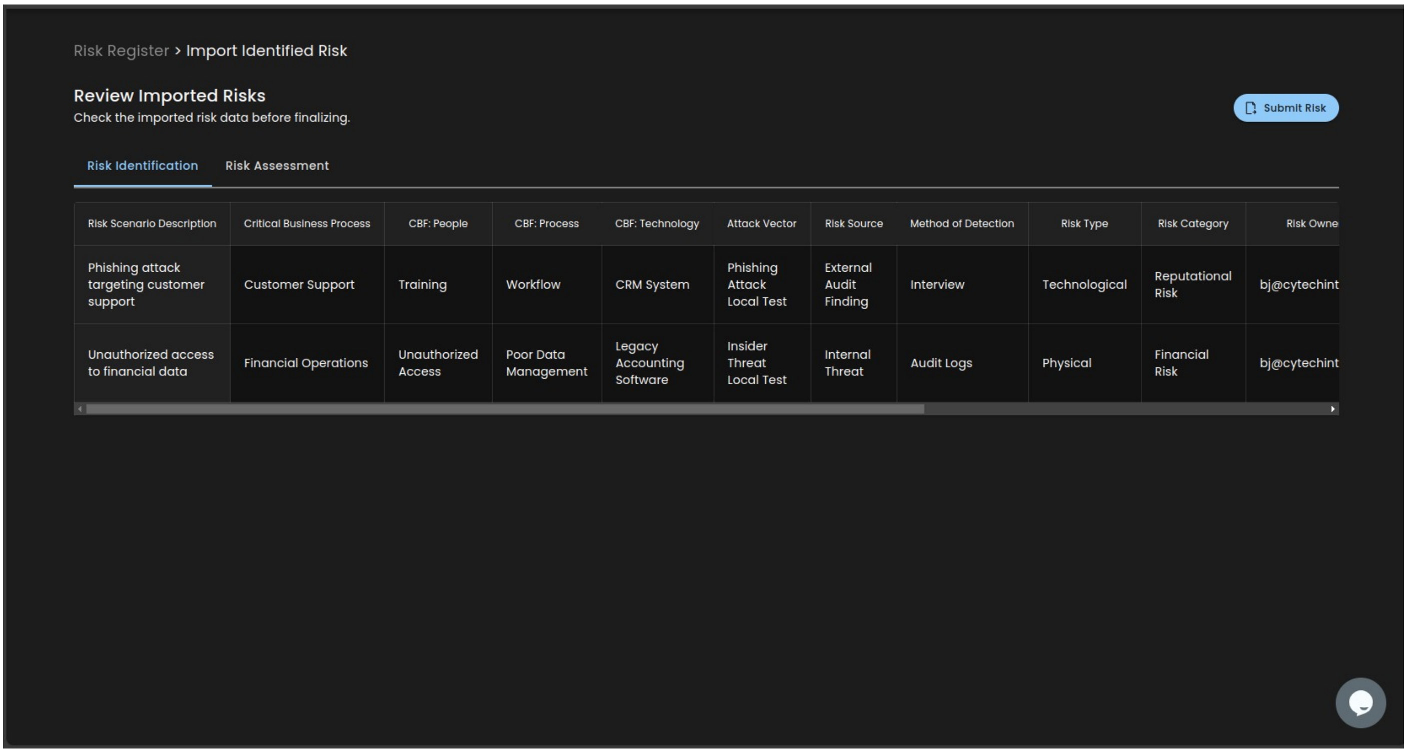
RM Import Improvements and Limitation Support



Risk Register > Import Identified Risk

Review Imported Risks

Check the imported risk data before finalizing.

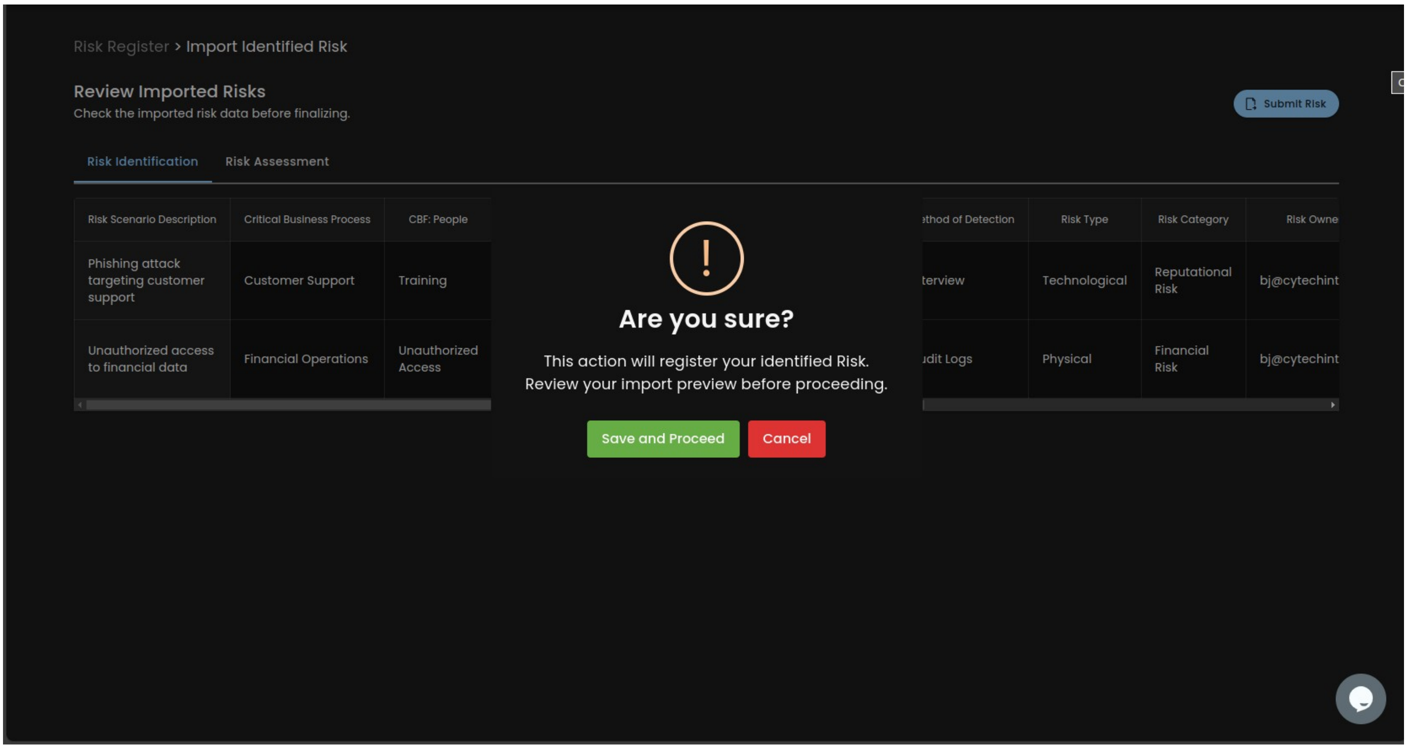


Risk Register > Import Identified Risk

Review Imported Risks

Check the imported risk data before finalizing.

Risk Scenario Description	Critical Business Process	CBF: People	CBF: Process	CBF: Technology	Attack Vector	Risk Source	Method of Detection	Risk Type	Risk Category	Risk Owne
Phishing attack targeting customer support	Customer Support	Training	Workflow	CRM System	Phishing Attack Local Test	External Audit Finding	Interview	Technological	Reputational Risk	bj@cytechint
Unauthorized access to financial data	Financial Operations	Unauthorized Access	Poor Data Management	Legacy Accounting Software	Insider Threat Local Test	Internal Threat	Audit Logs	Physical	Financial Risk	bj@cytechint



Risk Register > Import Identified Risk

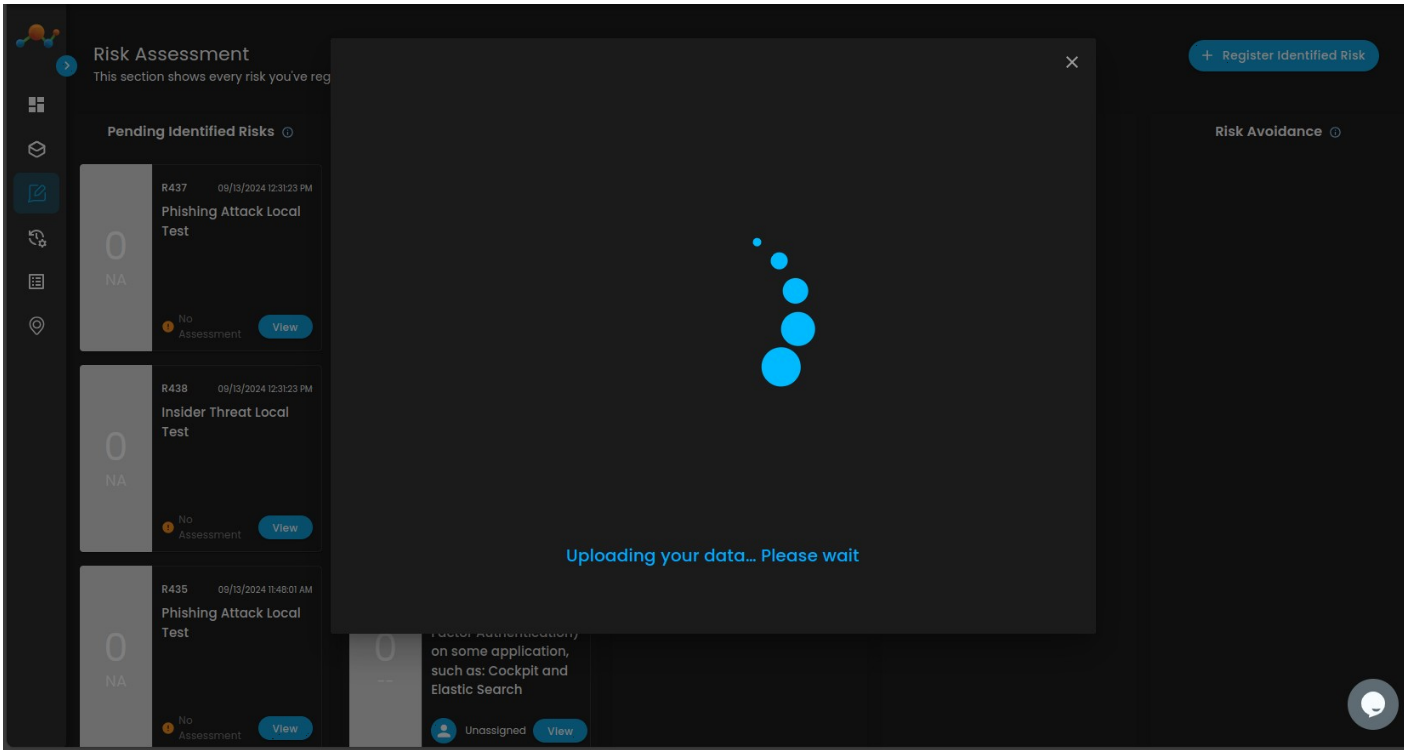
Review Imported Risks

Check the imported risk data before finalizing.

Risk Scenario Description	Critical Business Process	CBF: People	thod of Detection	Risk Type	Risk Category	Risk Owne
Phishing attack targeting customer support	Customer Support	Training	terview	Technological	Reputational Risk	bj@cytechint
Unauthorized access to financial data	Financial Operations	Unauthorized Access	udit Logs	Physical	Financial Risk	bj@cytechint

Are you sure?

This action will register your identified Risk. Review your import preview before proceeding.



Risk Assessment

This section shows every risk you've reg

R437 09/13/2024 12:31:23 PM Phishing Attack Local Test

R438 09/13/2024 12:31:23 PM Insider Threat Local Test

R435 09/13/2024 11:48:01 AM Phishing Attack Local Test

Factor Authentication) on some application, such as: Cockpit and Elastic Search

Uploading your data... Please wait

Revision #1

Created 13 September 2024 11:15:54 by Aldion Pueblos

Updated 14 September 2024 06:48:12 by Aldion Pueblos