


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.

View Team

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.

View Team

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.

View Team

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.

View Team

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.

View Team



BCM Create Team Role Forms

CISO Workplace

12:44 PM (UTC)

AP

Business Continuity Teams and Roles > Team Roles

Crisis Management

Last Updated: ##

Team Members

These are the Team Members of this Team.

Role	Responsibilities
------	------------------

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

Next

2 Primary Contact

3 Alternate Contact

Primary Contact Email

RACI

+ Add Member

0-0 of 0

Business Continuity Teams and Roles > Team Roles

Business Continuity Management

Last Updated: ##

Team Members

These are the Team Members of this Team.

+ Add Member

Role	Responsibilities	Primary Contact	Primary Contact Title	Primary Contact Email	RACI
IT DR Mgmt. Represen	Act as liaison with the IT DR Management Team.		CTO		

1-1 of 1

CIM Updates:

Alert Timeline Timestamp Fix in CIM-v3

Go back > Case: 10113

STEP 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.

Case Playbook

Alerts

Reports

Incident Response

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
03:48 PM

Timeline

Table Timeline

Jump to

Change layout

Change density

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
UserLoginFailed
User Name:
Host Name:
Source IP:
Destination IP:
Event Category:
Event Outcome: failure

11 Sep, 2024 @ 13:25:22

cytech-logcollector
UserLoginFailed
User Name:
Host Name:
Source IP:
Destination IP:
Event Category:
Event Outcome: failure

11 Sep, 2024 @ 13:24:42

Investigation Guide

Timeline Details

Table

Json File (Raw)

time

Title

Value

e365.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.

Drag & Drop or click to upload

Note:

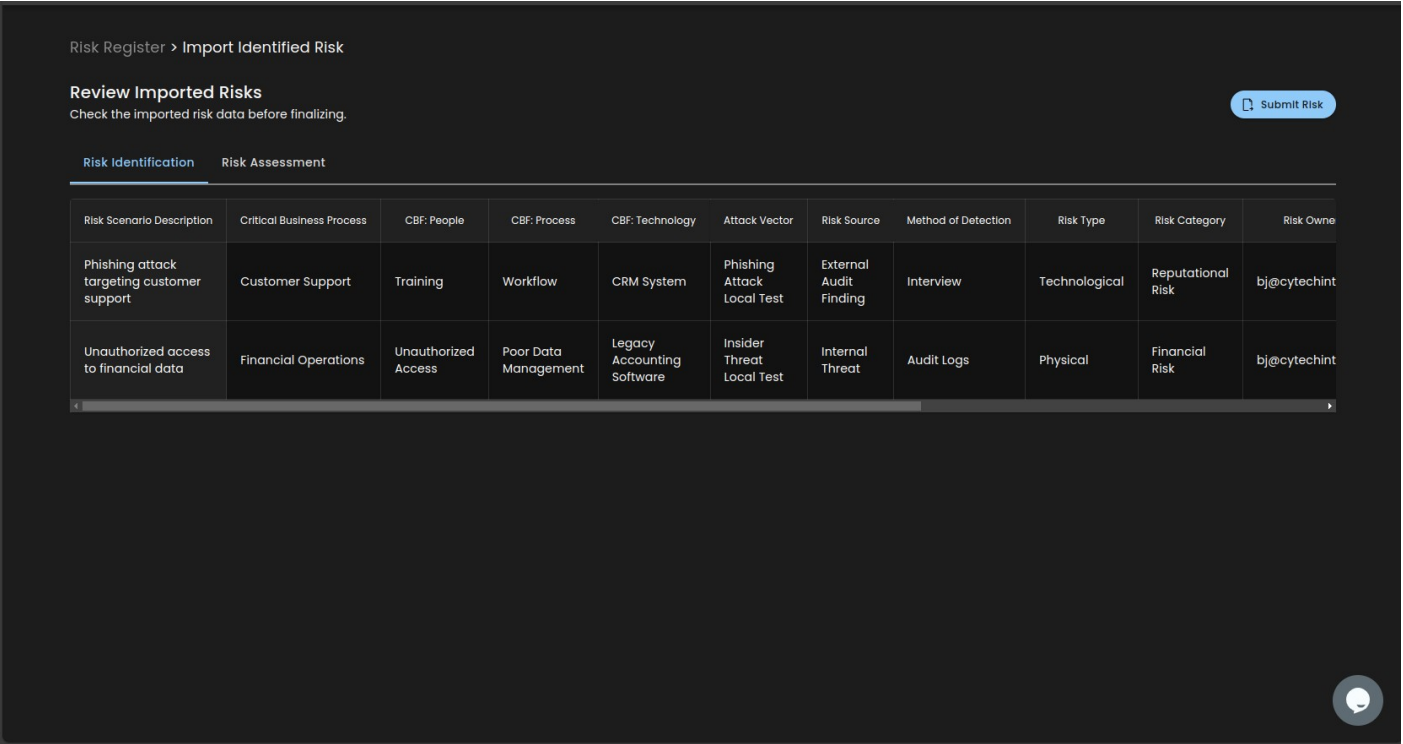
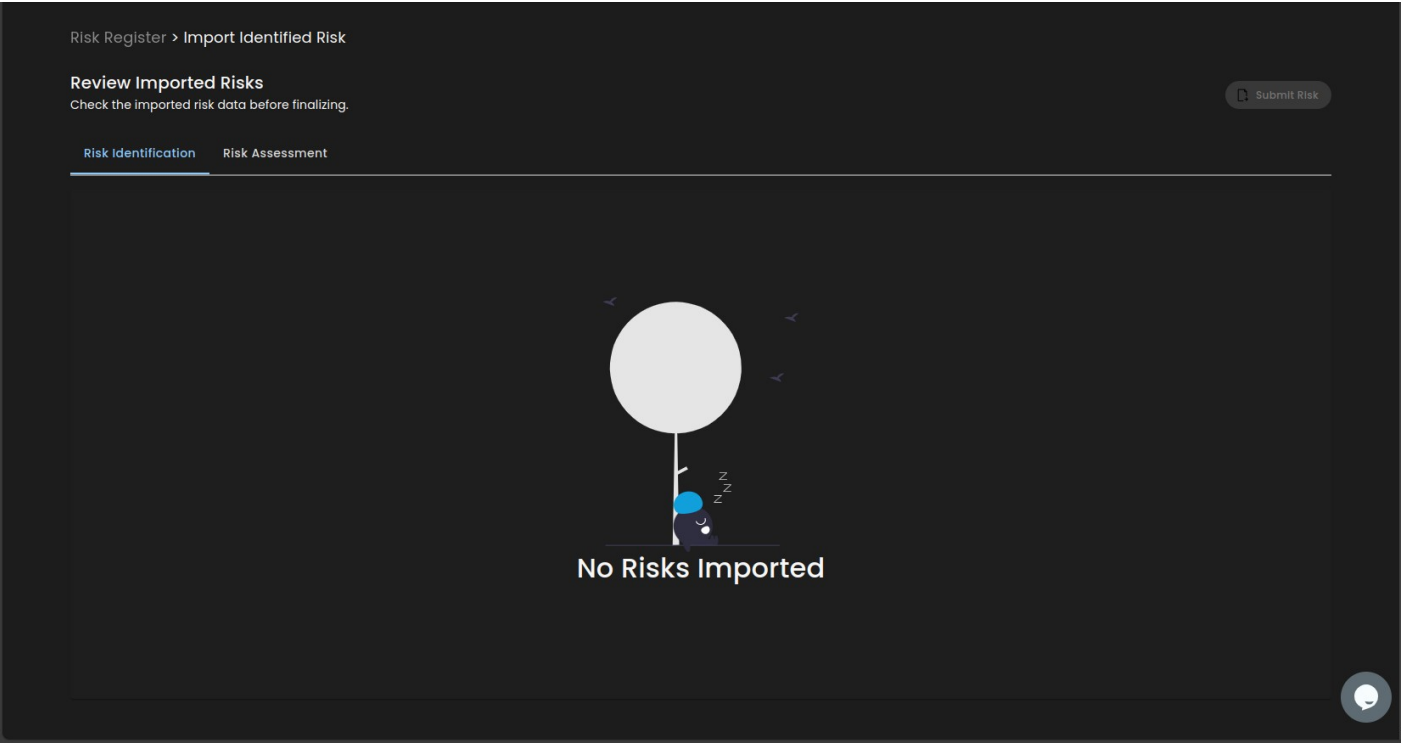
Make sure to use the provided [CyTech Template](#) for seamless importing of recipients.

Download CyTech Template for RM

Back

Finish

RM Import Improvements and Limitation Support



Risk Register > Import Identified Risk

Review Imported Risks

Check the imported risk data before finalizing.

Submit Risk

Risk Identification

Risk Assessment

Risk Scenario Description	Critical Business Process	CBP: People
Phishing attack targeting customer support	Customer Support	Training
Unauthorized access to financial data	Financial Operations	Unauthorized Access

Are you sure?

This action will register your Identified Risk.
Review your Import preview before proceeding.

Save and ProceedCancel

Method of Detection	Risk Type	Risk Category	Risk Owner
Interview	Technological	Reputational Risk	bj@cytechint
Audit Logs	Physical	Financial Risk	bj@cytechint

Risk Assessment

This section shows every risk you've reg

Pending Identified Risks

0

NA

R437

09/13/2024 12:31:23 PM

Phishing Attack Local Test

No Assessment

View

0

NA

R438

09/13/2024 12:31:23 PM

Insider Threat Local Test

No Assessment

View

0

NA

R435

09/13/2024 11:48:01 AM

Phishing Attack Local Test

No Assessment

View

0

NA

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

Unassigned

View

Register Identified Risk

Risk Avoidance

Uploading your data... Please wait