IT Risk Register

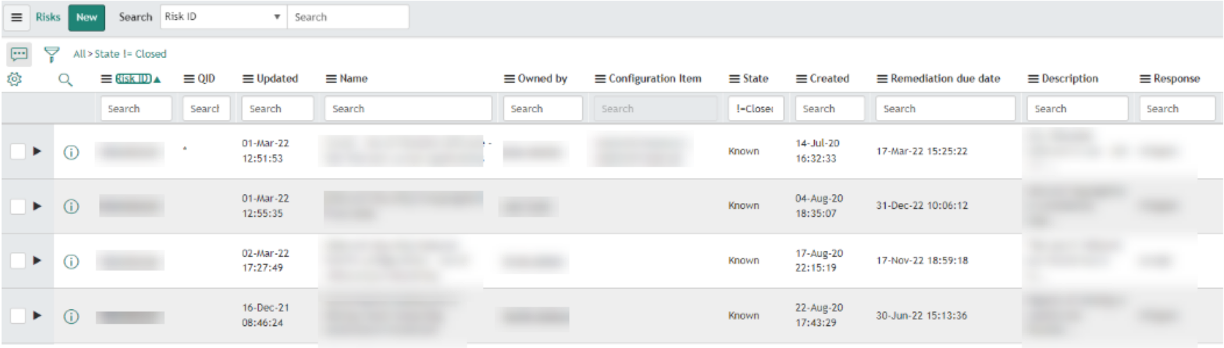
ZW Owned by Zshaquel Walker •••
Last updated: Apr 07, 2022 • 4 min read • 1 person viewed • Attachments • Legacy editor

Purpose of Risk Register

- A risk register acts as a central ledger to document all known and perceived IT Security Risks or vulnerabilities that could impact projects, processes or the business overall
- A well-maintained risk register may note when a risk event first occurred, how it was resolved and who was assigned to deal with it
- Allows us to analyze and categorize each identified threat by priority and which threats to address first
- It is useful to think of your risk register as a kind of knowledge arsenal that contains important instructions on overcoming known threats, addressing potential blind spots and avoiding common pitfalls

How We Manage Vulnerabilities Identified As Risks

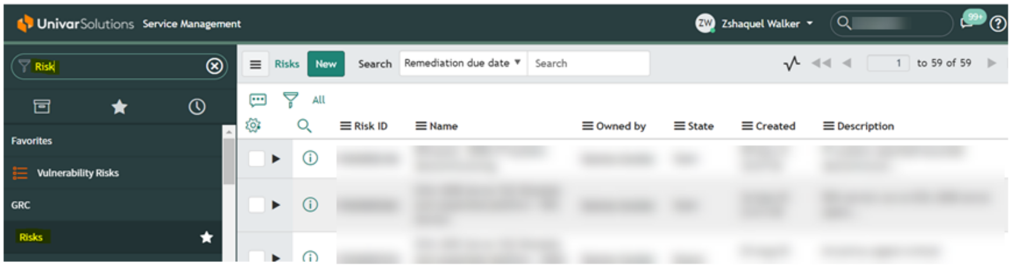
- Vulnerabilities are first scanned using the Vulnerability data base link to [redacted] to gather the data source
- Some vulnerabilities are identified and communicated to the IT Security team via email
- Once identified, the vulnerabilities are logged into the Risk Register for tracking
- The security team may work directly with system owners on a quick remediation or plan to remediate over quarterly maintenance cycle
- If we are unable to remediate after a reasonable period, we then add the vulnerability to the Risk Register for tracking



Risk ID ▲	QID	Updated	Name	Owned by	Configuration Item	State	Created	Remediation due date	Description	Response
Search	Search	Search	Search	Search	Search	!=Closed	Search	Search	Search	Search
[redacted]		01-Mar-22 12:51:53	[redacted]	[redacted]	[redacted]	Known	14-Jul-20 16:32:33	17-Mar-22 15:25:22	[redacted]	[redacted]
[redacted]		01-Mar-22 12:55:35	[redacted]	[redacted]		Known	04-Aug-20 18:35:07	31-Dec-22 10:06:12	[redacted]	[redacted]
[redacted]		02-Mar-22 17:27:49	[redacted]	[redacted]		Known	17-Aug-20 22:15:19	17-Nov-22 18:59:18	[redacted]	[redacted]
[redacted]		16-Dec-21 08:46:24	[redacted]	[redacted]		Known	22-Aug-20 17:43:29	30-Jun-22 15:13:36	[redacted]	[redacted]

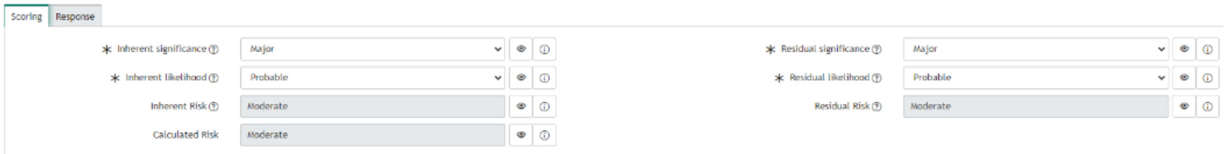
- Once a risk has been logged, it is assigned to the Manager of the team responsible for remediation response
    - The Risk Register can be reached at: [redacted]
    - Type "risk" at the filter navigator
    - Click on Risk

Note: [redacted] *approval may be required to access the register depending on the current SNOW GRC permission of the individual.*



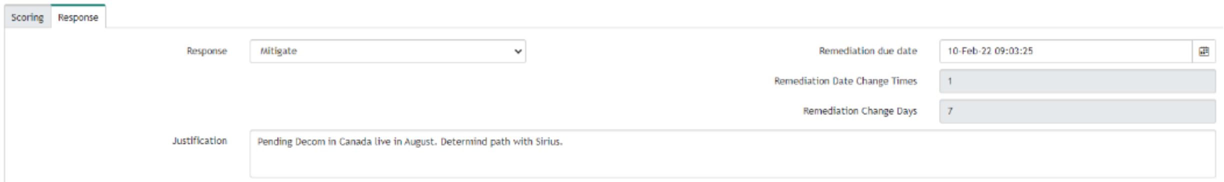
Risk ID	Name	Owned by	State	Created	Description
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

- Scoring of risk level and Response sections are to be updated and completed by the Risk Owner



* Inherent significance	Major	* Residual significance	Major
* Inherent likelihood	Probable	* Residual likelihood	Probable
Inherent Risk	Moderate	Residual Risk	Moderate
Calculated Risk	Moderate		

- Response, Remediation Due Date and Justification fields are to be completed in a timely manner by the risk owner
- Remediation task should be created and assigned to the person responsible for addressing the threat
- The risk owner/manager is responsible for assigning the remediation task and following through on resolution of the vulnerability or threat



Response	Mitigate	Remediation due date	10-Feb-22 09:03:25
		Remediation Date Change Times	1
		Remediation Change Days	7
Justification	Pending Decom in Canada live in August. Determind path with Sirius.		

Risk Responses

Avoid the risk by changing requirements for security or other system characteristics

Transfer the risk by allocating the risk to other systems, people, organizations, or assets; or by buying insurance to cover any financial loss should the risk become a reality

Mitigate the risk of severity or seriousness of an event using one of the below mitigation strategies:

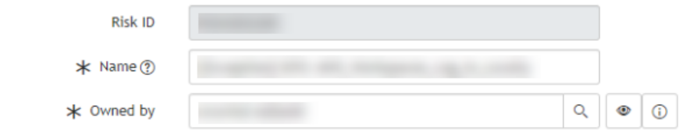
- Update and Upgrade Software Immediately
- Defend Privileges and Accounts
- Enforce Signed Software Execution Policies
- Exercise a System Recovery Plan
- Actively Manage Systems and Configurations
- Continuously Hunt for Network Intrusions
- Leverage Modern Hardware Security Features
- Segregate Networks Using Application-Aware Defenses
- Integrate Threat Reputation Services
- Transition to Multi-Factor Authentication

Accept indicates that the organization is willing to accept the level of risk associated with a given activity or process. Accept is only selected when risk owner plans to review the risk for "Exception" status.

Risk_Exceptions

A risk exception occurs when a particular policy, standard, security program requirement, or security best practice cannot be fully implemented.

A common exception may occur when a business or individual acknowledges that the potential loss from a risk is not great enough to warrant spending money to avoid it. Also known as "risk retention."

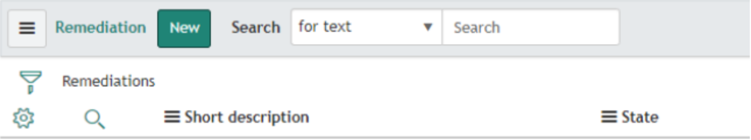


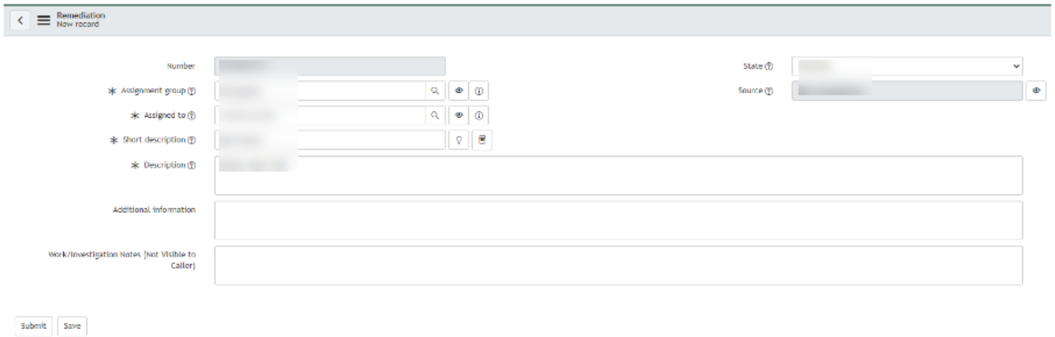
Risk ID	[redacted]
✱ Name ⓘ	[redacted]
✱ Owned by	[redacted]

Note: *Risk exceptions can only be approved by IT Leadership*

Remediation Tasks

- Remediation tasks should detail which group and person the task is assigned to
- Short and full description of the remediation plan for the specific task
- State of the work – Work in Progress, Pending, Closed Completed
- Work/Investigation Notes" section within the Remediation section should be maintained by the risk owner





Number	[redacted]	State ⓘ	[redacted]
✱ Assignment group ⓘ	[redacted]	Source ⓘ	[redacted]
✱ Assigned to ⓘ	[redacted]		
✱ Short description ⓘ	[redacted]		
✱ Description ⓘ	[redacted]		
Additional information			
Work/Investigation Notes (Not Visible to Caller)			

Note: *Risks approaching or exceeding remediation are reviewed monthly.*

Note: *Policy (GPO related exceptions are a separate process).*

Closing Risk

Once remediation has completed, the risk owner is asked to log final activities within the risk, confirm response status is "Mitigate" and move risk status to "Closed.

+ Add label

Related pages ⓘ

Measuring Risk
IT Compliance
Organized together

IT Security Assessment Process
IT Compliance
Organized together

Vulnerability Management and Policy Compliance Dashboards
IT Compliance
Organized together

Organized together

Organized together

Organized together

IT Compliance
IT Compliance

Organized together

Information Security
IT Compliance

Organized together

2021-12-14 Security Assessment Criteria and Email Notification Meeting notes
IT Compliance

Organized together

👍 👏 🎉 ☺ Be the first to add a reaction

ZW Write a comment...