

Within every RiskWatch risk management product is a powerful and flexible Risk Register that allows you to easily catalog and rank threats and risks to your organization.

Identify and evaluate your risks from all threats that can potentially negatively impact your organizations. Assign ratings to whatever metrics you would like to use that can include impact, likelihood, criticality, exposure, and any others. These ratings can be qualitative or quantitative, with a customizable scoring system.

If you assess multiple areas, for example physical security and cyber security, you can have separate registers for each type of area that you assess.

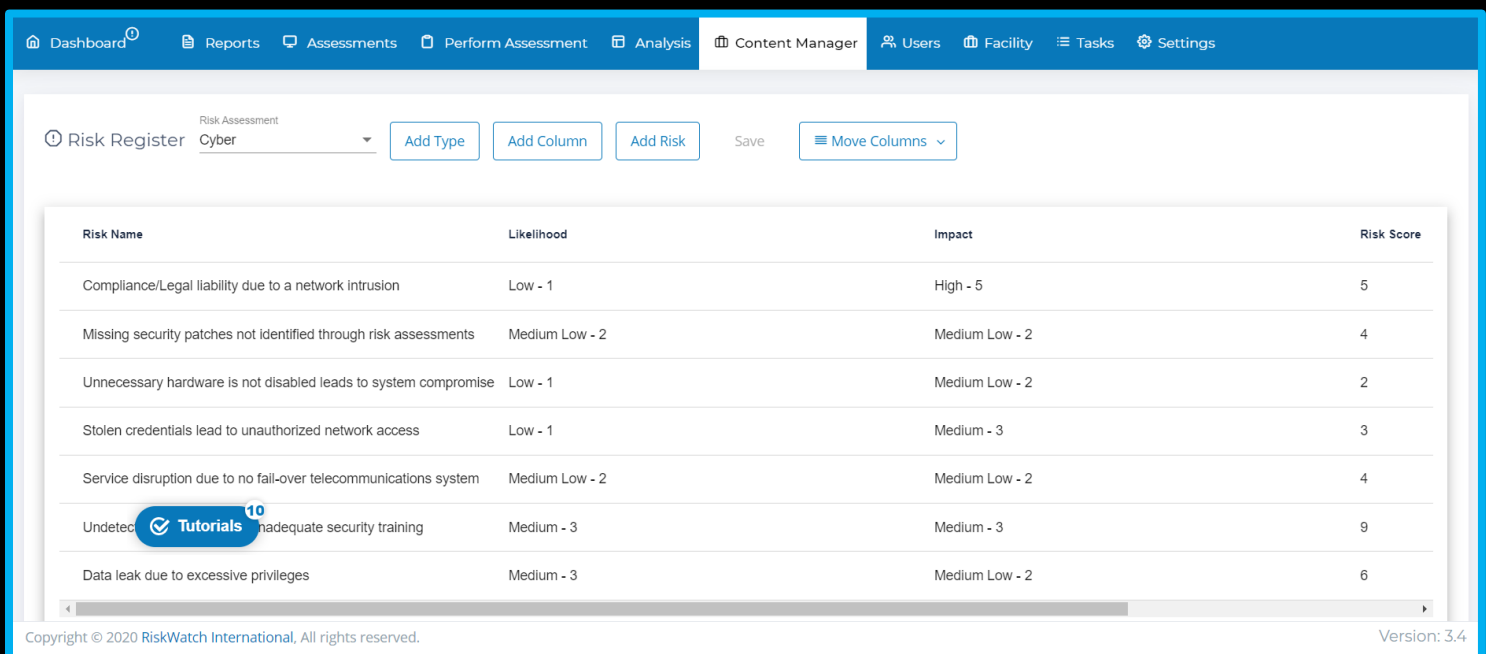
Additionally, the risk register can pull data from assessment surveys. For example, you can use survey questions to be answered by members of your organization to determine the likelihood value for each threat.

Use the application's automated report tool to generate a polished report of your risk register. Make it a stand-alone report or add you risk register to other reports generated through the application.

Adaptable to your security program

- Unlimited use cases
 - ✓ Cyber Threats
 - ✓ Physical Threats
 - ✓ Environmental Threats
 - ✓ Safety/Health Threats
 - ✓ Legal Threats
 - ✓ etc.
- Qualitative, Quantitative, or Semi-Quantitative
- Customizable metrics and terminology
- Customizable risk score calculations
- Customizable data fields

Sample basic qualitative cyber risk register



The screenshot shows the RiskWatch Risk Register interface. The top navigation bar includes Dashboard, Reports, Assessments, Perform Assessment, Analysis, Content Manager, Users, Facility, Tasks, and Settings. The main content area shows a Risk Register for 'Cyber' with a table of risks. The table has columns for Risk Name, Likelihood, Impact, and Risk Score. A 'Tutorials' badge is visible over the table. The footer contains copyright information and the version number 3.4.

Risk Name	Likelihood	Impact	Risk Score
Compliance/Legal liability due to a network intrusion	Low - 1	High - 5	5
Missing security patches not identified through risk assessments	Medium Low - 2	Medium Low - 2	4
Unnecessary hardware is not disabled leads to system compromise	Low - 1	Medium Low - 2	2
Stolen credentials lead to unauthorized network access	Low - 1	Medium - 3	3
Service disruption due to no fail-over telecommunications system	Medium Low - 2	Medium Low - 2	4
Undetected inadequate security training	Medium - 3	Medium - 3	9
Data leak due to excessive privileges	Medium - 3	Medium Low - 2	6