



SIMPLERISK – TRANSFORMING RISK MANAGEMENT. SIMPLE. AUTOMATED. EFFECTIVE

## How to Perform an Internal Risk Assessment in SimpleRisk

### Introduction

In this short video, we will review how to leverage the CIS Critical Security Controls assessment in SimpleRisk as an excellent way to perform a basic risk assessment for your organization.

We've included a template for CIS in SimpleRisk that contains 20 yes/no answer questions that shouldn't take you more than a few minutes, but will provide valuable insight into your organization's risk posture.

### Instruction

To begin the process, from the menu at the top of SimpleRisk, click on "**Assessments**" and then select "**Critical Security Controls**" under the **Available Assessments**. You can leave the "**Asset Name**" field blank, or enter the name of a specific application or business unit to which your answers will apply.

Below is a screen shot of the Critical Security Controls assessment.

A screenshot of the SimpleRisk web application showing the "Critical Security Controls" assessment form. The top navigation bar includes "Risk Management", "Asset Management", "Assessments", "Reporting", and "Configure". The "Assessments" menu is open, showing a list of options: "Available Assessments", "Pending Risks", "Create Assessment", "Edit Assessment", and "Send Assessment". The "Create Assessment" option is selected. The main form area is titled "Critical Security Controls" and contains a text input field for "Asset Name". Below this are six questions, each with "Yes" and "No" radio button options. The questions are: 1. Do you actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access? 2. Do you actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution? 3. Do you establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings? 4. Do you continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers? 5. Do you have processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications? 6. Do you collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack? 7. Do you minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and emails systems?

From here, simply answer "Yes" or "No" to the 20 questions and click on "**Submit**". A risk will be created for each "No" answer under the "**Pending Risks**" section found on the left. Click on "**Add**" to push the risks into SimpleRisk.



This concludes the video on “How to Perform an Internal Risk Assessment” in SimpleRisk. If any questions were left unanswered or could use more in-depth descriptions, please submit your feedback to our Customer Support email address which is [support@simplerisk.com](mailto:support@simplerisk.com)