



# Ostrich

Cyber-Risk

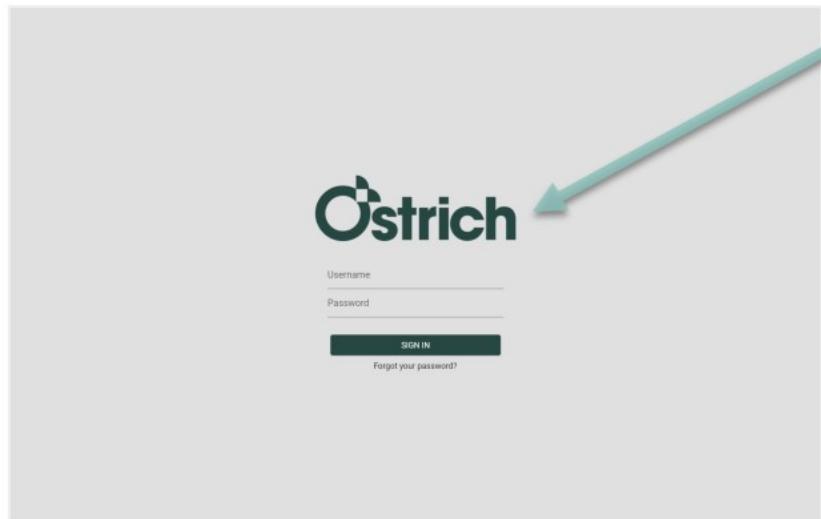
## User Guide

# Table of Contents

Introduction .....	1
Assessments .....	2
Targets .....	3
Analysis .....	4
Reports .....	5
Business Units .....	6
Users.....	7

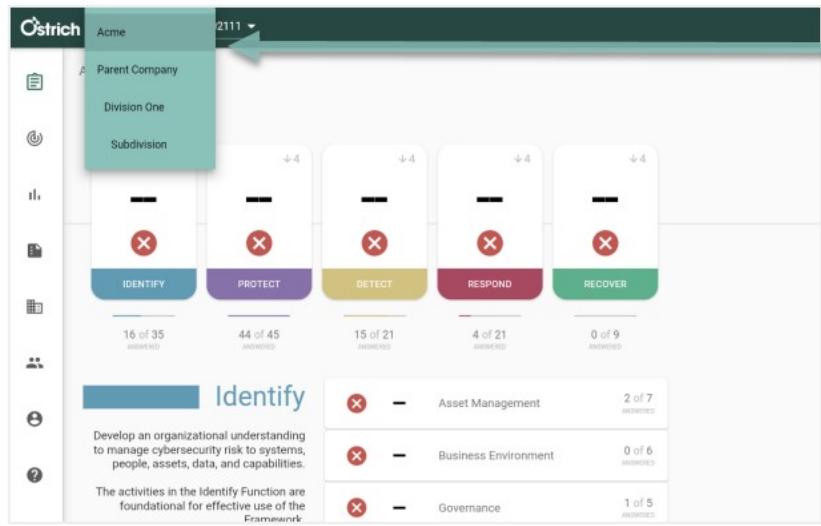
# Getting Started

Login page and business unit selection



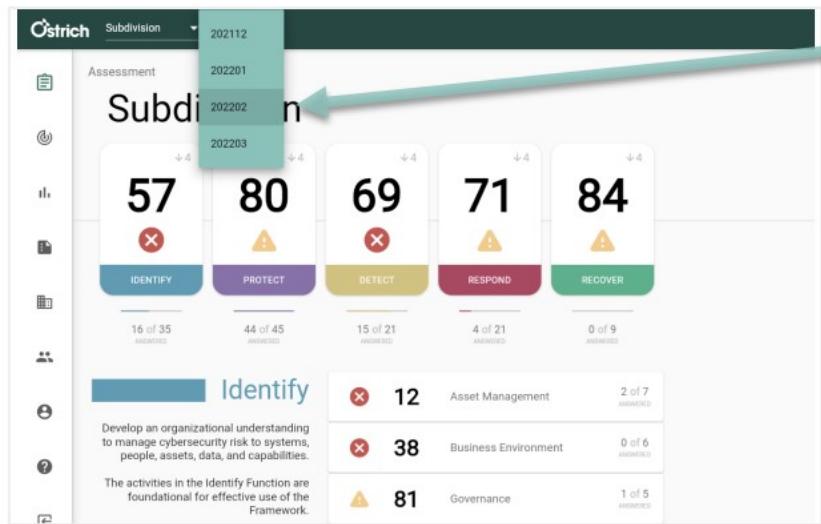
1

Logging in is simple. Your username is the email address associated with your account. You should have received an email prompting you to set your password.



2

Make sure the correct company is selected in the top left of the page. A different company/business unit may be selected from the drop-down menu.

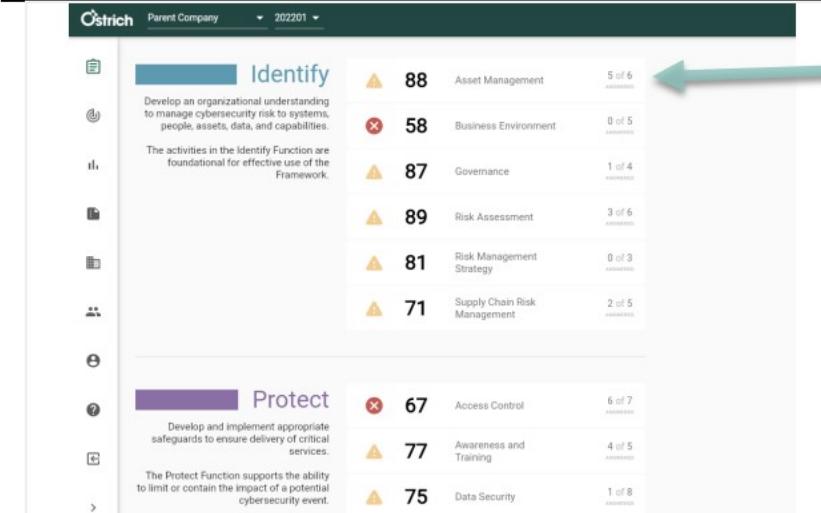
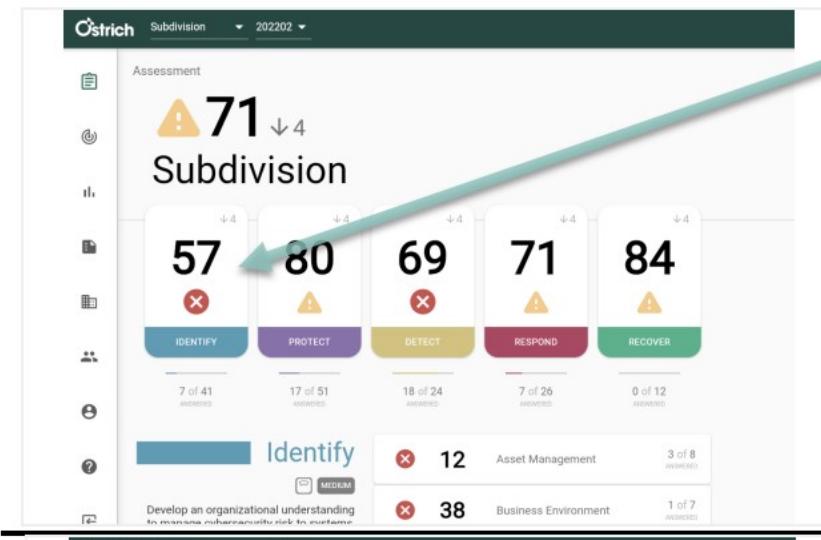


3

Select the period for your assessment from the drop down menu.

# Assessment

Steps to take to evaluate your company



Assessment > Identify > Asset Management

ID.AM-1 Physical devices and systems within the organization are inventoried

REFERENCES

- CIS CSC 1
- COBIT 5 BA09.01, BA09.02
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-3-2:2013 SR 7.8
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
- NIST SP 800-53 Rev. 4 CM-8, PM-5

PROCESS

I do not have the appropriate information or expertise to answer this.

No inventory

Manual inventory

Automated inventory planned

Automated inventory being built

Automated Inventory

Automated and audited inventory

1

In this tab there are six scores. An overall score and five NIST section scores. Click on any of the NIST Scores (e.g. Identify) to jump to a break down of your score for the section.

2

The overall score for Asset Management is broken down into subcategories. Selecting a score activates a test.

3

Answer the questions according to the controls you have in place to get an accurate assessment.

# Targets

Questions used to determine your company's goals for its security

The Targets section displays a company average score of 64 for Subdivision. Below this, five specific targets are listed with their respective scores and answer counts:

Target	Score	Answers
IDENTIFY	67	14 of 41 ANSWERED
PROTECT	65	25 of 51 ANSWERED
DETECT	57	19 of 24 ANSWERED
RESPOND	59	2 of 26 ANSWERED
RECOVER	75	0 of 12 ANSWERED

A large green arrow points from the company average score of 64 down to the Identify target score of 65.

1

The Targets section contains a similar layout to the Assessment section. There are six scores with the first being a company average. Click on the Identify section to delve deeper into the settings.

The Identify section shows the overall score of 74 for Asset Management, broken down into six categories:

Category	Score	Answers
Asset Management	49	4 of 6 ANSWERED
Business Environment	76	0 of 5 ANSWERED
Governance	50	2 of 4 ANSWERED
Risk Assessment	79	1 of 6 ANSWERED
Risk Management Strategy	91	1 of 3 ANSWERED
Supply Chain Risk Management	74	1 of 5 ANSWERED

2

The overall Identify section score is broken down into the controls here. Clicking on any section inside this tile will bring you to the controls used for measuring and weighing.

This tool measures the company's current security to the vision of the perfect (or preferred) security set up. You can change the weight of any target as well as set the goal you would like to reach.

ID.AM-1 Physical devices and systems within the organization are inventoried

REFERENCES

- CN-CRC-1
- CORIT 5 AM-09-01, R499.02
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-3-3:2013 SR 7.7.8
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
- NIST SP 800-53 Rev. 4 CMA, PM-5

PROCESS

This question does not apply to this business unit.

How critical or relevant is this to our organization?

LOW MEDIUM HIGH

Which answer represents our goal or needs?

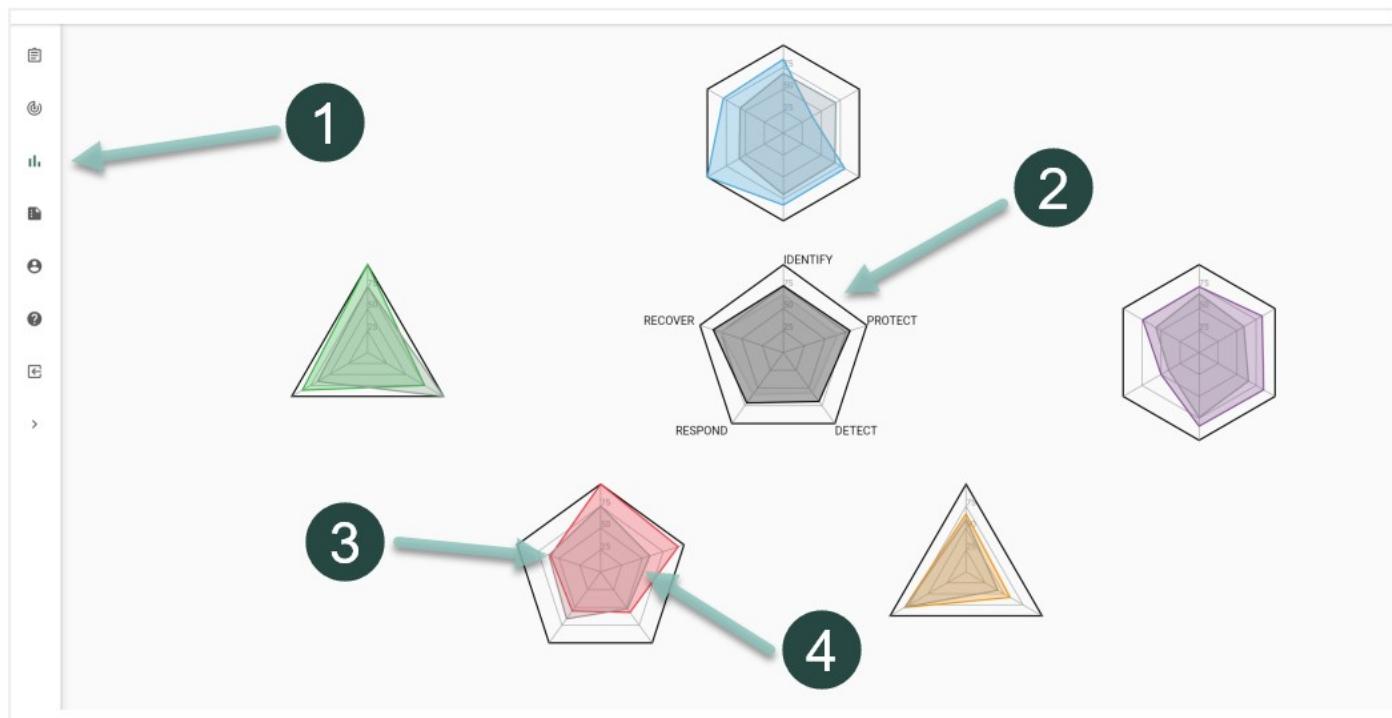
- No inventory
- Manual inventory
- Automated inventory planned
- Automated inventory being built
- Automated inventory
- Automated and audited inventory

3

This tool measures the company's current security to the vision of the perfect (or preferred) security set up. You can change the weight of any target as well as set the goal you would like to reach.

# Analysis

Spider charts to visualize progression



1 The Analytics tab

2 The central spider chart shows how close the company is to its targets. Each of the corners point to a corresponding spider chart that breaks down the section.

3 In the colored spider charts, the colored indicators show what the company is doing to hit its goals: green is assigned to Recover, red to Respond, yellow to Detect, and so on.

4 The gray section of the colored spider charts is a visualization of the company's goals. The colored section should overtake the gray section as your company improves its security.

# Reports

Generate reports to share risk posture

The screenshot shows the Ostrich platform interface with the 'Reports' tab selected. The top navigation bar includes a back arrow, the 'Ostrich' logo, a 'Subdivision' dropdown set to 'Subdivision', and a date range dropdown set to '202203'. On the left, there's a vertical sidebar with icons for file management, users, and help. The main content area displays a 'Generate PDF Report – Subdivision (202203)' button at the top. Below it, a section titled 'Previously Generated Reports:' lists three reports: 'Company Branch 2 Report - 202201' (generated on February 24, 2022, 7:45 PM), 'Risk Team Report - 202201' (generated on February 24, 2022, 7:44 PM), and 'CEO Report - 202202' (generated on February 24, 2022, 6:30 PM). Each report entry has a download icon to its right. Two green arrows point from numbered callouts to specific elements: one arrow points from '1' to the download icon of the first report, and two arrows point from '2' to the date stamps of the second and third reports.

Generate PDF Report – Subdivision (202203)

Previously Generated Reports:

- Company Branch 2 Report - 202201      February 24, 2022 7:45 PM
- Risk Team Report - 202201      February 24, 2022 7:44 PM
- CEO Report - 202202      February 24, 2022 6:30 PM

1

Go to the Reports tab to see reports generated for each period. Click the download button to generate and open a report. Inside you can see what recommendations to put in place to improve your NIST score.

2

Date stamps indicate when a report was generated. Click the download button to download a past version of the report.

# Users

*List of users by email with their assigned roles*

Users		
superuser	practitioner_assessments	
1	2	
superuser	practitioner_assessments	
@ostrichcyber-risk.com	:	
superuser	practitioner_assessments	
superuser	practitioner_reports	practitioner_assessments
superuser	practitioner_reports	practitioner_assessments

1

A list of users along with the roles you have assigned to them will be found in the Users tab.

2

Click the three dots to add roles to a user. A user must be assigned the Practitioner Assessments role in order to take assessments and the Practitioner Reports role in order to be able to generate reports.