

Birdseye Assess - Simplify Your Risk Assessments

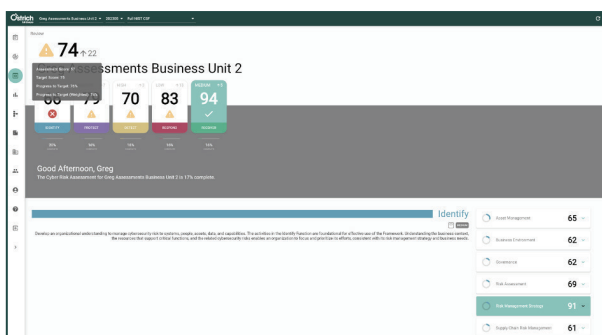
Replace manual spreadsheets with a collaborative assessment dashboard.

A comprehensive SaaS solution using a consistent and repeatable assessment methodology based on proven industry-standard security frameworks.

What Makes Birdseye Assess Different

1. NIST CSF assessment framework with references to other best standards (NIST 800-53, ISO 27001, CIS 18, COBIT, and ISA 62443) to measure your security program control strength.
2. MITRE ATT&CK enterprise framework assessment tailored for financial services.
3. Run unlimited assessments across the whole organization or divisions and compare results.
4. Customize assessments to measure progress toward your business objectives.

Birdseye Assess Screenshots



Birdseye Assess Dashboard

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

Guidance
CIS CONTROLS 1.1: Establish and Maintain Detailed Asset Inventory
Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IOT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

[Less info](#)

REFERENCES

- COBIT 2019 BAI09.01, BAI09.02
- ISA 62443-2-1:2009 A.2.3.4
- ISA 62443-3-3:2013 SR 7.8
- ISO/IEC 27001:2022 A.8.1.1, A.8.1.2
- NIST SP 800-53 Rev. 5 CM-8, PM-5
- CIS CSC 1

PROCESS

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

No inventory of physical devices and/or systems within the organization exists.

A manual inventory of physical devices and/or systems within the organization exists.

An automated inventory of physical devices and/or systems within the organization is being planned.

An automated inventory of physical devices and/or systems within the organization is being built.

An automated inventory of physical devices and/or systems within the organization has been implemented.

NOTES

Enter Notes

Laptops/Office Devices
Evidence Link: Asset_Inventory

Last edited by: IV

COVERAGE

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

What portion of the devices and systems are inventoried?

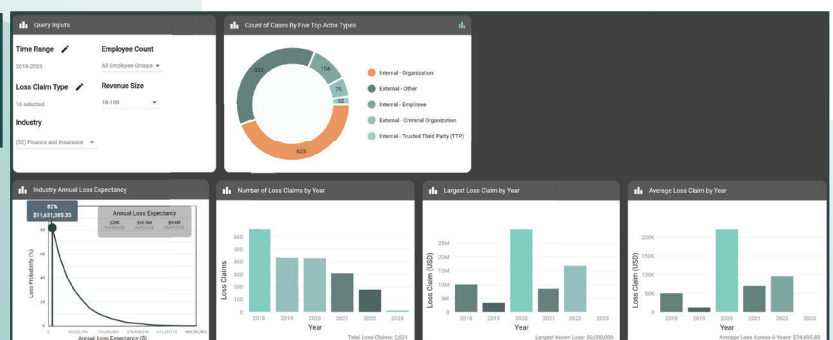
0% 100%

NOTES

Enter Notes

NIFT CSF Assessment with guidance and references

Benchmark data for your industry and size based on historic insurance loss claims



How Birdseye Assess Works:

1. Perform periodic qualitative assessments of your cybersecurity program using an intuitive assessment workflow to leverage our collection of frameworks.
2. During the assessment, Birdseye will evaluate and score the current state of each control and measure your progress to your desired target goals.
3. Once complete, this assessment will be the foundation for establishing the maturity for your cybersecurity program, allowing you to focus on improving controls with lower scores that fall short of your business objectives.

The Value of Birdseye Assess Across the Organization



Review risk exposure for your industry based on Insurance Loss Claims over the last 15 years



Private Equity/Venture Capital:
Assign assessments to portfolio companies to ensure they meet control targets



Library of risk assessment profiles, like ransomware, cloud workloads or priority controls for cyber insurers to benchmark against industry standards and peers



Assign assessments to 3rd party vendors to assess supply chain risk



Collaborate with multiple subject matter experts to complete an assessment



Built-in program management with consistent and repeatable assessment workflows



To learn more about other Ostrich Cyber-Risk offerings, visit www.ostrichcyber-risk.com or contact info@ostrichcyber-risk.com