

Insider Threat CMMI Assessment

Protecting Trade Secrets (proprietary data)

LeastTrust & .ai

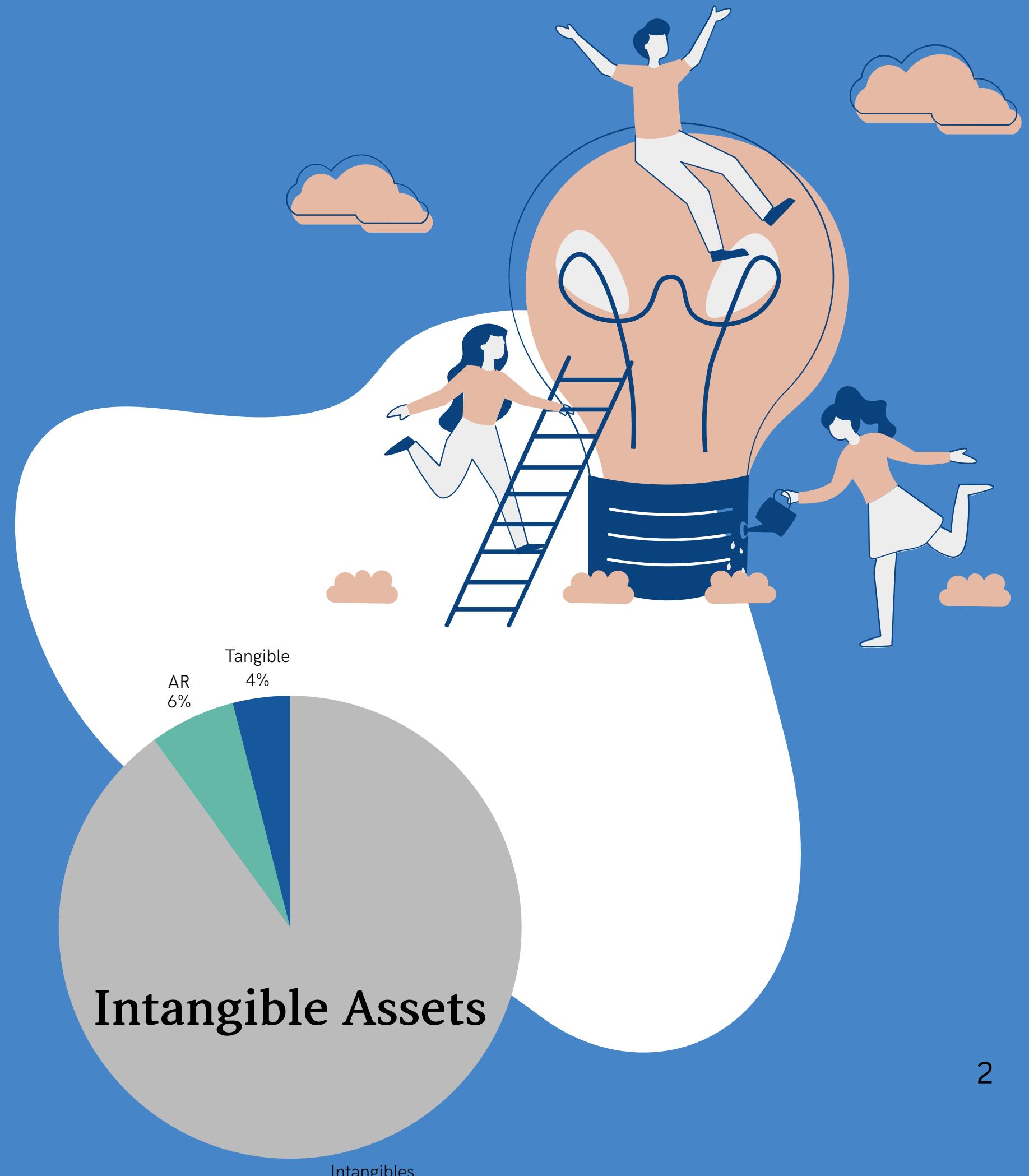


Risk

90% of your company's value is intangible and a large share residing in data.

Employees take *confidential and proprietary data to their next job

*legal term - trade secrets



Trade Secrets

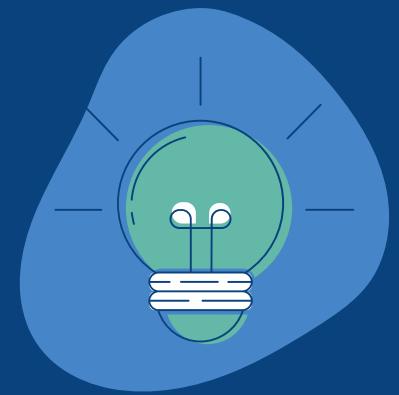
All organizations have trade secrets.

Trade secrets are more than the recipe for Coca Cola





The employee creates
or joins a competitor



Stolen data might help a
competitor erase your
market headstart, erode
market share, set
optimal pricing, or
improve the product



What are your
defenses?

Uncapped Damages

Proprietary edge erased



Organizations have no incentive to disclose an insider breach

FBI Internet Crime Report

1% is proprietary (IP) data theft

VBIR - Verizon Breach Incident Report

No Note of Insider Threat

Privelege Misuse - Less than 2% is
malicious Insider

No ISAC or Open Source Insider Intelligence

Why CMMI?

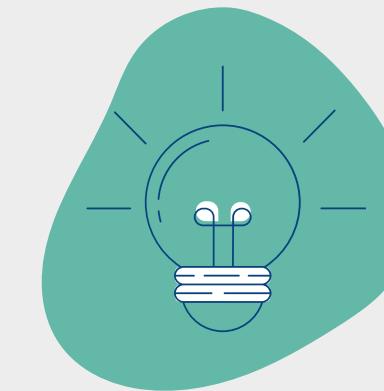
Combining Counter-Intelligence,
Cybersecurity, TPRM, Legal, HR, and
Governance best practices to
expose/validate our clients defenses



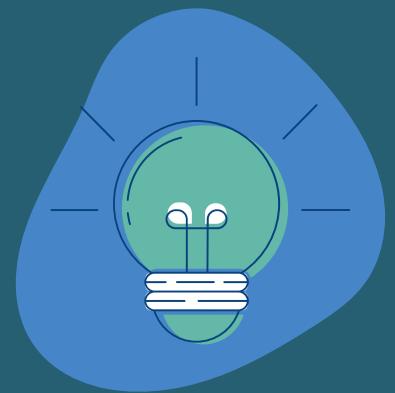
Over 400 questions



Working backward
from trade secret
litigation



Control validation in
the absence of open-
source threat
intelligence



Federal Law - Defend
Trades Secrets Act
(DTSA)



State Law - All States
have laws on trade
secret protection



Employment Laws -
Violation of employment
agreements

Legal Remedies

In general, to constitute a trade secret under these various laws (which each have their own nuances), the information must (1) have economic value; (2) because it is not generally known; and (3) the owner has taken reasonable measures to keep the information a secret.

Case Lessons

Top 3 reasons cases fail:

1. The plaintiff failed to sufficiently identify the trade secret
2. failed to protect the trade secret,
3. or never legally contracted an obligation to the employee

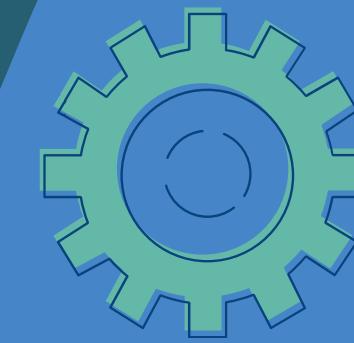


Non Technical Controls

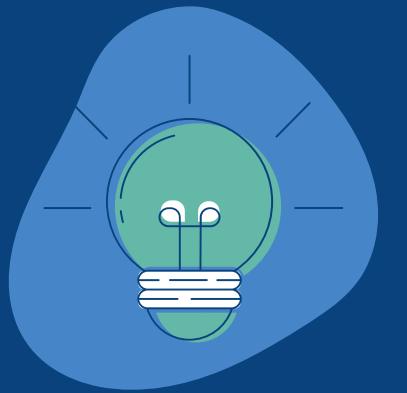


Contract Clauses, NDAs,
Onboard & Exit
Procedures, Employee
Training

Technical Controls



Email Monitoring, Managed
Browser, “Warning”
Deterrents, Access Reviews,
Alerts, Logging, Rule
Creation,



Planning:
Architecture,
Governance, & Policy
Creation



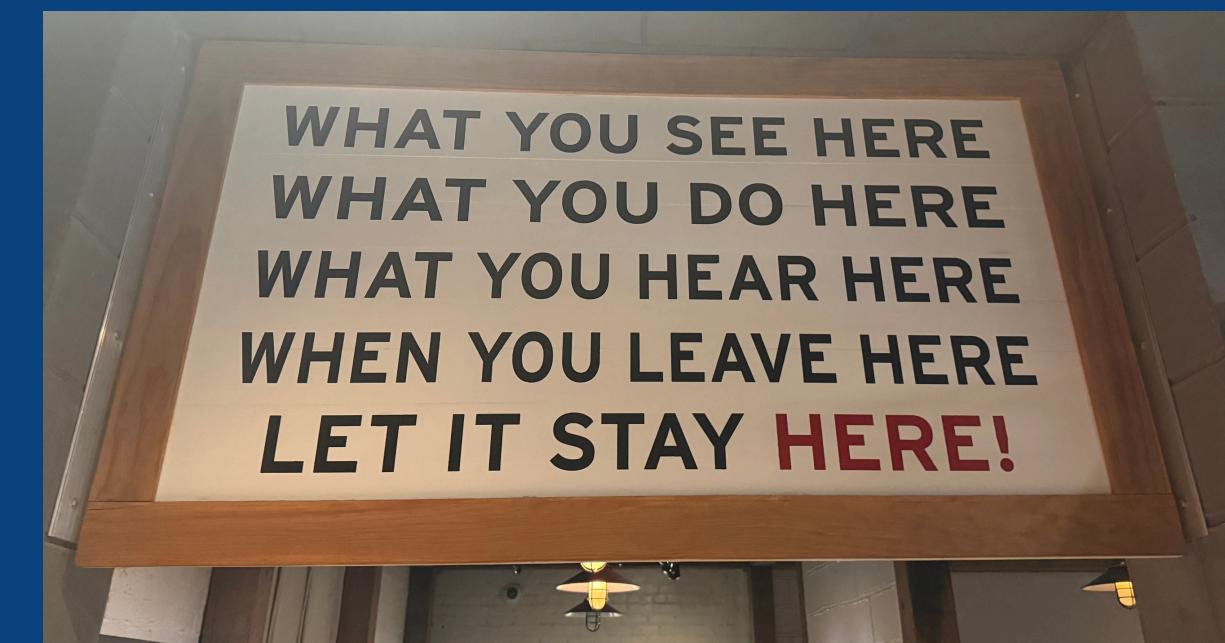
Integrate and Train



Enforce, Manage,
Iterate, Measure, &
Improve with Tools

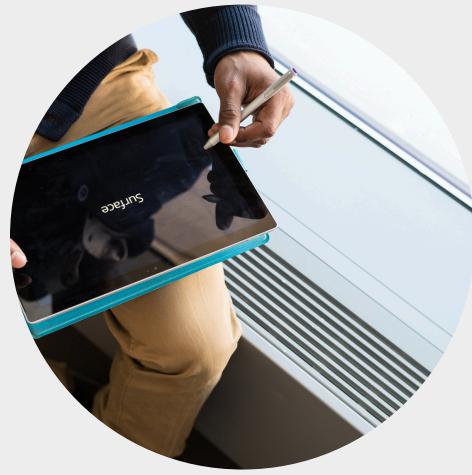
Insider Threat Program

How can an organization build reasonable defenses to protect its sensitive data?



Assessment Process

Plan, Interview, Send



Scheduling or Self Exam



Uno/LeastTrust Contact
and Nudging



Scoring and Followups



Report Issued / Strategy
Workshop

Uno.AI Platform

Planning & Compliance Backbone

- Coordination
- Governance
- Framework Alignment
- Scheduling
- Questions
- Guidance
- Evidence
- Metrics Review

The screenshot shows the Uno.AI Platform's web interface. The top navigation bar includes icons for user profile, notifications, and a location, followed by the text "Least Trust IT". The main menu has tabs for Entities, Risks, Controls, Assessments (which is selected), Attachments, and Exceptions. On the left, there's a sidebar with various icons and a search bar. The main content area is titled "Assessments" and "Questions". It features a "Search" bar and buttons for "+ Add a Question" and "Upload Question Set". A table lists two questions:

| Question | Answer Guideline | Question Type | Tags | Question Required? | Attachment Required? |
|-----------------------------------------------------------------------------------|------------------|---------------|--------------|--------------------|----------------------|
| Have you established someone who is ultimately responsible for data security? | Input text | Text | + Assign Tag | False | False |
| What metrics do you use to measure data protection effectiveness on a time basis? | Input text | Text | + Assign Tag | False | False |

Detailed Questions

- Initial Question
- Dependency followup questions

✓ L.4 : Understanding the Control

⚠ Response text area must be filled out

Question * Can you describe the organization's approach to re-screening employees, and how it is aligned with the principles of Least Trust and Trade Secret Assurance Framework? (Required: Explanation, approximately 100-150 words) Example: "The organization has a periodic re-screening process in place for all employees, which includes re-running background checks and re-evaluating financial and personal information. This process is designed to identify potential risks and ensure that employees continue to meet the organization's security and trust standards."

Answer

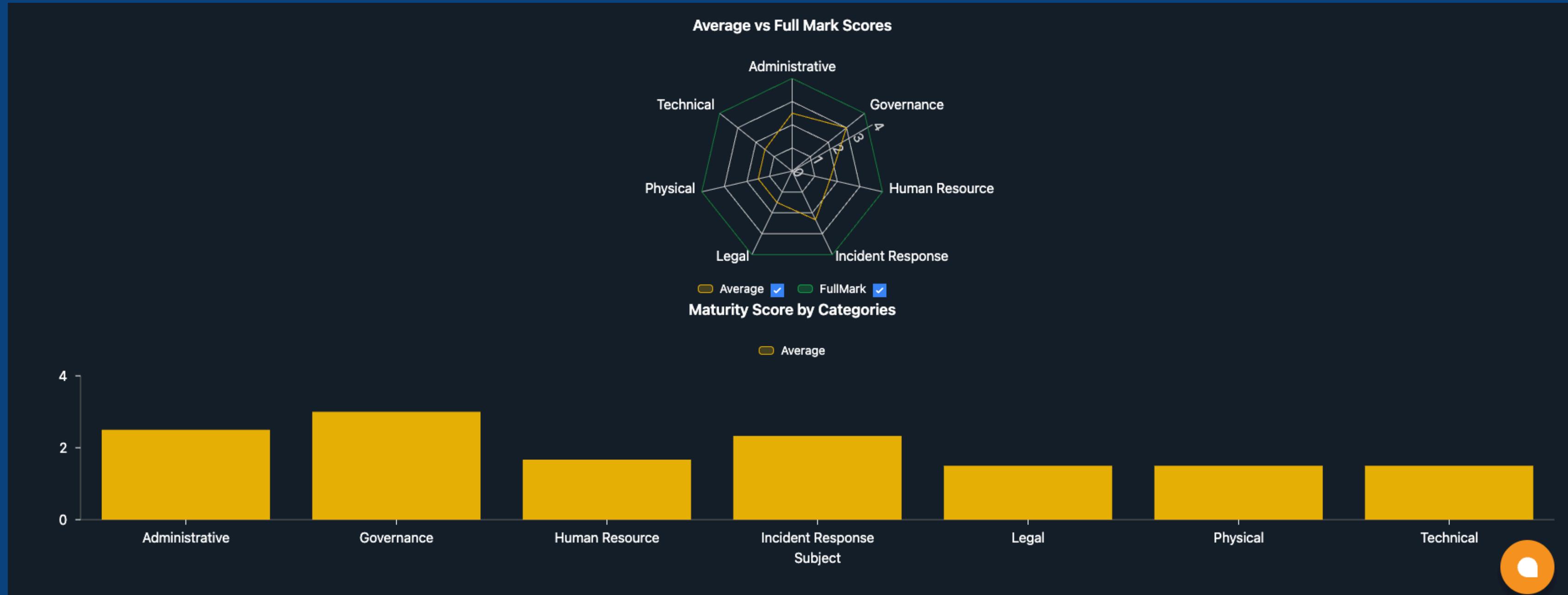
⚠ Response text area must be filled out

Question * What triggers a re-screening of an employee? (Required: List of triggers) Example: "Re-screening is triggered by events such as: (1) annual anniversaries, (2) significant changes in job responsibilities, (3) reports of suspicious behavior, or (4) drastic life changes (e.g. sudden wealth or financial difficulties)"

Answer

CMMI Report

- Prioritized recommendations per department
- Ability to re-weight to your risk register



Sample Analysis

← Assessments / Maturity

H.4 Tier 2

Companies should be creative to support incentives for championing proprietary data protection and valuable IP. Incentives include rewards for process improvements, consistent awareness testing results, and creation of large amounts of classified proprietary data

Tier (Maturity level)

Tier 2 — Repeatable

Observations

- Program existence:** The respondents describe a Quarterly Innovation Awards Program and a Security Champions Program, indicating a formal incentive structure is in place.
- Program scope:** The awards list includes multiple tiers (Bronze, Silver, Gold, Innovator of Year) and a quarterly schedule, suggesting some level of program maturity.
- Management involvement:** Quarterly meetings with the CISO are mentioned, implying that senior management is engaged.
- Recognition mechanisms:** Awards are monetary, certificates are issued, gift cards are provided, and quarterly meetings add a non-monetary element. This demonstrates a diversity of reward types.
- Metrics/continuous improvement:** Participation data (8.7% in 2024) and the number of awards (47) are reported, and the organization states it plans 2025 enhancements to broaden participation and deepen metrics.

Analysis & Conclusions

- Criterion 1 (existence):** A program is clearly described. 2 points are assigned because the program is articulated with award tiers, participation figures, and an organized schedule.
- Criterion 2 (comprehensiveness):** The presence of a CISO in quarterly meetings and reported award counts demonstrates some dedicated management and metrics, but the documentation does not detail a dedicated program manager or formal effectiveness metrics. 1 point is awarded.
- Criterion 3 (multiple recognition mechanisms):** Multiple reward types exist, yet integration with performance reviews or patent/trade-secret specific awards is not mentioned. 1 point.
- Criterion 4 (continuous improvement):** The organization cites planned improvements and participation goals, indicating ongoing refinement, but lacks evidence of formal survey or brainstorming processes. 1 point.
- Total score:** 5 points, qualifying for Tier 2 (Repeatable).

Improvement Areas

- Define a dedicated program owner** – appoint a specific role (e.g., Innovation Incentives Manager) to coordinate award data, metrics, and continuous improvement activities.
- Integrate incentives into performance reviews** – embed award criteria into annual reviews to ensure alignment with business objectives and reinforce security awareness.
- Add formal metrics** – track additional KPIs such as the number of security-related suggestions accepted, reduction in data-breach incidents, or training completion rates linked to incentive eligibility.
- Implement structured feedback loops** – conduct quarterly employee surveys and brainstorming sessions focused on protection practices, using the findings to refine incentive criteria and award tiers. }

Sample Analysis

← Assessments / Maturity

T.10 Tier 0

Establish visual warnings (watermarks on critical documents), access review summary emails, and pop-ups (toasts) that remind or warn users of the mishandling of sensitive data. Tools such as Harmonics Security and the Enterprise Managed browser may have this functionality. Also overlaps with DRM

Tier (Maturity level)

Tier 0 — Partial to None

Observations

- Answers focus on the classification accuracy of Microsoft Purview Information Protection and the manual review of certain document types.
- No mention of visual warnings such as watermarks, pop-ups (toasts), or access review summary emails.
- There is no evidence provided for any of the deterrent mechanisms required by Control T.10.
- The organization indicates an awareness of the need for classification but does not describe deterrent deployment.

Analysis & Conclusions

- Tier 0 criteria require absence of any visual warnings, pop-ups, or summary emails and an overall lack of deterrent strategy.
- The provided responses satisfy all three elements of Tier 0: no deterrent implementations, no evidence of such mechanisms, and no evidence of understanding or planning regarding deterrent usage.
- Therefore the maturity level for Control T.10 is Tier 0.

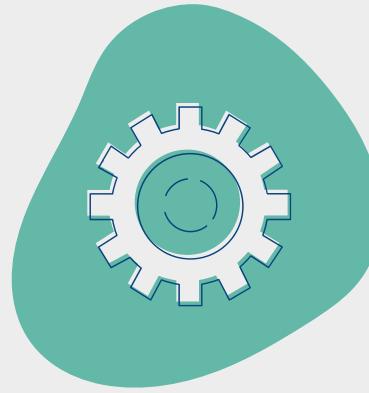
Improvement Areas

- Document the implementation** of visual warnings (watermarks on documents flagged as Confidential or higher) and provide sample screenshots.
- Deploy context-aware pop-ups** that trigger when users access or manipulate highly sensitive content.
- Establish recurring access-review summaries** sent to data owners and stakeholders; document the frequency and format.
- Integrate with DRM solutions** to ensure that protection extends beyond visual deterrence.
- Measure effectiveness** through user surveys or monitoring of deterrent interactions and iterate based on findings.
- Provide personalized data-access summaries** to each employee to reinforce accountability.
- Collect and retain evidence** (configuration files, audit logs, training materials) to support future assessments.

Pricing & Engagement Flexibility

We strive to add value to your team and workflows. Let us know how we can better position our resources.

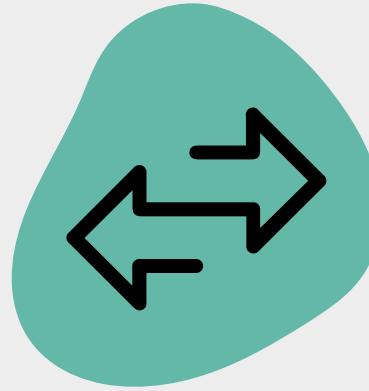
We value our “Insider Champions”



\$8,000 for platform and 20 hours labor: plan, interview, assess, workshop



Additional hours - \$300 per hour. (*No clients have exceeded as of yet)



Flexible to self-assess and dictate our role

Summary

Direct or self-assess ability with interview orchestration



Review and consult with LeastTrust at the clients option



Validate or expose new risks and controls for Insider Threat

