HITRUST CSF v11.7 Baseline Change FAQ

Changes to the e1 and i1in v11.7

With the release of v11.7, HITRUST is making changes to the e1 and i1 baselines. These adjustments are the result of multiple analysis focused on optimizing the e1 and i1 assessments.

Removal from current e1 baseline:

1223.09ac1System.1 [1203.1] – "Access to audit trails / logs is safeguarded from unauthorized access and use."

Why are we removing this requirement from the e1 baseline?

Based upon our cyber threat adaptive analysis CVID 1203.1 does not directly contribute to cyber threat coverage in the e1 baseline. Our cyber threat coverage measure is based on mappings from the requirement statements in the CSF to the Mitigations defined in the MITRE ATT&CK framework.

Also, restricting access to users on a need-to-use basis is broadly covered by e1 requirement CVID 0035.0. CVID 1203.1 expands on access restrictions by focusing on restrictions to access logs specifically, so while it is a best practice and included in the i1, it is not an essential practice.

NOTE: This requirement statement is still part of the i1 baseline.

Replacement in the current e1 and i1 baselines:

What is being replaced?

CVID 0501.0 is being replaced with CVID 3207.0 in the e1 and i1 baselines.

1403.05i1Organizational.67 [0501.0] – "Access granted to external parties is limited to the minimum necessary, limited in duration, and is revoked when no longer needed."

14.05i1Organizational.3 [3207.0] – "The organization ensures all third-parties with access to the organization's information or information systems meet contractual commitments for information security. The organization reviews independent assessments of all third-parties with access to its information or information systems to determine the suitability of the third parties' information security practices (e.g., security certification, attestation, or audit report, verification) at least annually."

Why are we replacing this requirement?

CVID 0501.0 does not directly contribute to cyber threat coverage based on MITRE Mitigation mappings and the historical results of our cyber threat adaptive analysis.

Additionally, CVID 0501.0 currently represents our Third Party Assurance domain in the e1. However, the focus of the requirement is more on controlling access by third parties and less on managing the risk associated with third parties. We considered moving CVID 0501.0, but the domain for Access Control would not benefit from the additional scope specificity of CVID 0501.0 due to existing requirements addressing the limitation of access.

We also considered incorporating an existing requirement from our Third Party Assurance domain into the e1 and i1 baselines. However, while our framework includes requirements addressing the monitoring of third-party compliance with contractual provisions, those requirements exceed the rigor expected from an 'essential' requirement. As such, we created a new requirement (CVID 3207.0) to represent the Third Party Assurance domain that contains only the essential elements needed for the e1.

Modification to requirements in the current e1/i1 baseline:

19180.09z1Organizational.2 [1103.0]

Current: The organization designates individuals authorized to post information onto a publicly accessible information system and trains these individuals to ensure that publicly accessible information does not contain nonpublic information.

Updated: The organization trains individuals to ensure that publicly posted information does not contain nonpublic information. If the organization permits the posting of information onto a publicly accessible information system, it designates individuals authorized to post the information.

Why are we making this modification?

Our goal with this modification is to clarify the intent of CVID 1103.0 and reduce the number of requirements that are not applicable to customers. Rather than focus on designation of individuals as the primary component of the requirement, we are shifting the focus onto training all individuals to prevent data leakage.

16.09l1Organizational.4 [2326.0]

Current: The organization maintains offline and/or immutable backups of data.

Updated: The organization maintains offline and/or immutable backups of data for an organization defined period of time.

Why are we making this modification?

The modification to CVID 2326.0 is to clarify our position on its implementation. Maintaining offline and/or immutable backups remains one of the most effective ways to reduce the impact of cyberattacks. Because the relevance of backup data can vary based on an organization's operations, each organization should establish and document its own criteria for how long such backups remain relevant and maintain them in alignment with that determination.