Eligibility and Background

Who is eligible to perform a HITRUST AI Security (ai1 or ai2) assessment?
Providers of Artificial Intelligence (AI) systems, including AI application providers and AI platform providers, are eligible to perform an ai1 or ai2 assessment.

Who is considered an AI provider?
Per ISO/IEC 22989:2022, an AI provider is an organization or entity that provides products or services that uses one or more AI systems, which encompasses:

- AI platform providers: Provide services that enable other organizations to deliver AI-enabled products or services.
- AI product providers: Provide AI-enabled products directly usable by end-user / end-customer.

What types of AI models qualify to be assessed?
Generative AI, predictive AI (i.e., non-generative machine learning), and rule-based AI (i.e., expert systems) models qualify to be assessed.

How many AI security requirement statements will be added to the assessment?
No more than 44 AI security-specific HITRUST CSF requirements will be added to an assessment, depending on how the assessment is tailored.

Which AI security threats were considered in developing the assessment?
HITRUST considered a total of 13 threats in developing the assessment. For more information about the threats please visit HITRUST AI Hub page.

Assessment

Is the ai1 or ai2 assessment a stand-alone assessment?
No, the ai1 or ai2 assessment must be added to a HITRUST e1, i1, or r2 validated assessment.

Do I have to create a separate standalone assessment object within MyCSF to perform an ai1 or ai2 assessment?
No, the ai1 or ai2 assessment is added to an existing e1, i1 or r2 assessment object.

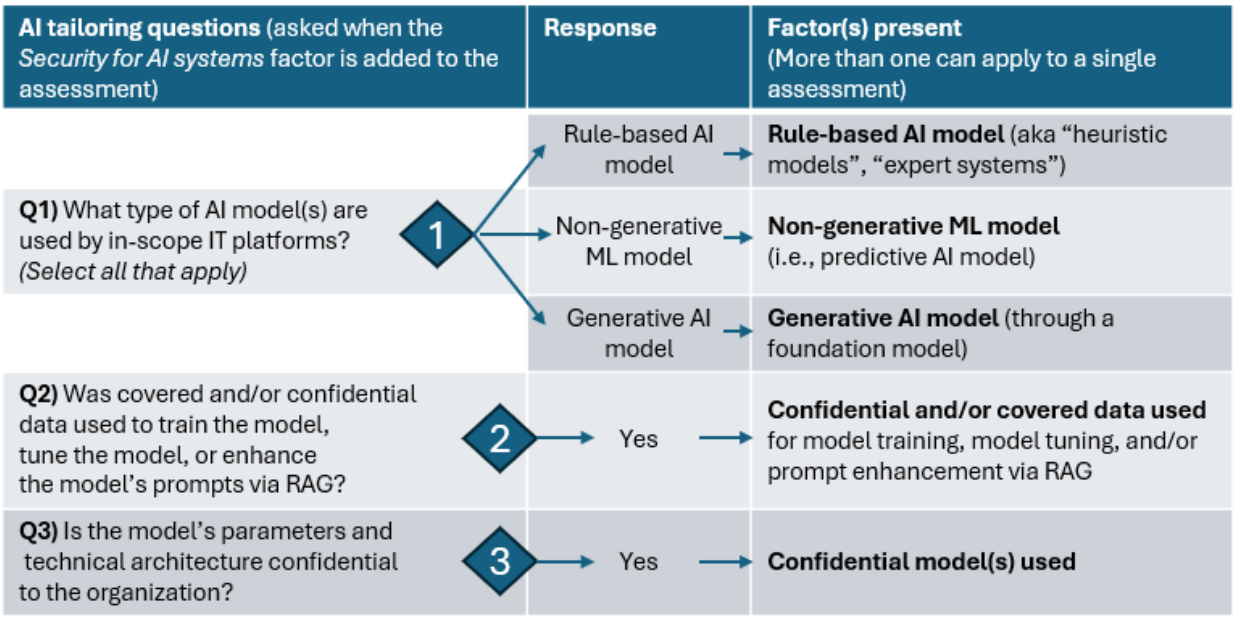
Is HITRUST requiring that the Security for AI Systems compliance factor be added to my HITRUST e1, i1, or r2 assessment if my in-scope IT platforms use AI?
No, the ai1 or ai2 assessment is an optional add-on that HITRUST strongly recommends, but does not require, adding to an e1, i1, or r2 assessment when AI is leveraged within the scope of the HITRUST assessment.

Which control maturity levels are required to be assessed in an ai1 or ai2 assessment?
For an a1 assessment, the "Implemented" control maturity level must be assessed. For an a2 assessment, the "Policy", "Procedure" and "Implemented" control maturity levels must be assessed. The "Measured" and "Managed" control maturity levels may optionally be scored in an ai2 assessment.

What types of HITRUST assessments qualify?
Validated and readiness e1, i1, or r2 assessments using CSF v11.4.0 and later that are tailored to include the Security for AI Systems compliance factor.

Are there any new assessment tailoring questions for AI in MyCSF?
Yes. The three questions listed below would need to be answered when the Security for AI Systems compliance factor is included in an e1, i1 or r2 assessment.

The tailoring questions are:



Where can I find definitions of the Security for AI Systems compliance factor?
Please visit the MyCSF help Site.

Which assessment domains have AI security requirements?
The following domains have AI security requirements:

- 01 Information Protection Program
- 06 Configuration Management
- 07 Vulnerability Management
- 09 Transmission Protection
- 11 Access Control
- 12 Audit Logging & Monitoring
- 13 Education, Training and Awareness
- 14 Third Party Assurance
- 15 Incident Management
- 16 Business Continuity & Disaster Recovery
- 17 Risk Management
- 19 Data Protection & Privacy

Inheritance

Can any of these AI security requirements be inheritable from AI platform/application providers?
Yes, inheritability is supported. Inheritance can be requested in the same manner as it is requested for e1, i1 or r2 assessment. Please visit the References page in MyCSF to access the most current Shared Responsibility Matrices for inheritance providers.

Report Credits

Do I need to purchase the ai1 or ai2 assessment report credit before booking my QA reservation?
No. Only the e1, i1 or r2 validated report credit is required to book a QA reservation.

Do I need to purchase the ai1 or ai2 assessment report credit before I submit my assessment to HITRUST?
Yes.

Do I need an ai2 assessment report credit for the interim assessment?
No.

Certification Thresholds, CAPs and Gaps

How will the certification threshold be calculated for the ai1 or ai2 assessment?

ai2 assessment:

- For the underlying r2 assessment, all domains must have a straight-average minimum score of 62, inclusive of the AI security requirements.
- The average control maturity scores of all AI security requirement statements tailored into the assessment through the Security for AI Systems compliance factor must also achieve a minimum score of 62.

Example:

Requirement Statement from Domain 01	Core r2 Requirement Statement	Mapped to ai2 Assessment	Score included in Average Domain Score Calculation for r2 Certification	Score included in Average Score Calculation for ai2 Certification	Requirement Statement Scoring
Requirement Statement 1	Yes	No	Yes	No	75%
Requirement Statement 2	Yes	No	Yes	No	50%
Requirement Statement 3	Yes	No	Yes	No	100%
Requirement Statement 4	Yes	No	Yes	No	75%
Requirement Statement 5	No	Yes	**Yes**	Yes	100%
Requirement Statement 6	No	Yes	**Yes**	Yes	75%
Domain Average used for r2 CSF Certification Determination					**79.2%**
Average used for ai2 Certification Determination					**87.5%**

ai1 assessment:

- For the underlying e1 or i1 assessment, all domains must have a straight-average minimum score of 83 which is based only on the core e1 or i1 requirements. statements. Requirement statements added based upon compliance factors, such as Security for AI Systems, are not considered in average domain score calculation.
- The average control maturity scores of all AI security requirement statements tailored into the assessment through the Security for AI Systems compliance factor must also achieve a minimum score of 83.

Example:

Requirement Statement from Domain 01	Core e1 or i1 Requirement Statement	Mapped to ai1 Assessment	Score included in Average Domain Score Calculation for e1 or i1 Certification	Score included in Average Score Calculation for ai1 Certification	Requirement Statement Scoring
Requirement Statement 1	Yes	No	Yes	No	100%
Requirement Statement 2	Yes	No	Yes	No	100%
Requirement Statement 3	Yes	No	Yes	No	100%
Requirement Statement 4	Yes	No	Yes	No	75%
Requirement Statement 5	No	Yes	**No**	Yes	100%
Requirement Statement 6	No	Yes	**No**	Yes	75%
Domain Average used for e1 or i1 CSF Certification Determination					**93.8%**
Average used for ai1 Certification Determination					**87.5%**

How are CAPs and Gaps calculated for the ai2 assessment?

r2 assessment:

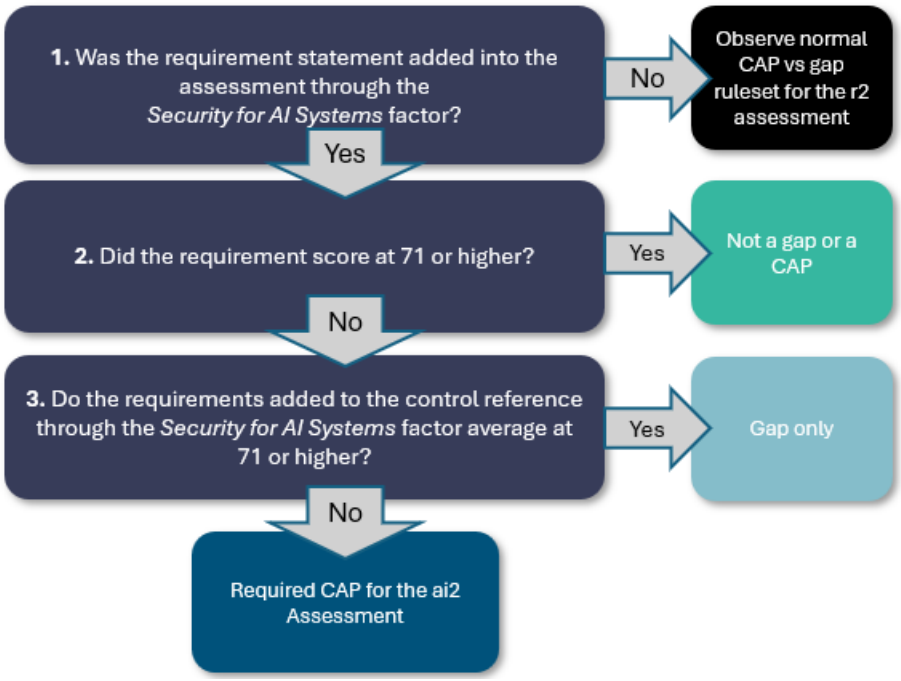
The following diagram illustrates the process for identifying CAPs and Gaps in an r2 assessment.

Example of an r2 assessment with a CAP and Gap:

Requirement Statement	Core r2 Requirement Statement	Mapped to ai2 Assessment	Associated Control Reference Require for Certification	CAP	Gap	Requirement Statement Scoring
11AA.09L1System.2	Yes	No	Yes	Yes	No	50%
11AB.09L1System.2	Yes	No	Yes	No	No	75%
11AC.09L1System.2	Yes	No	Yes	No	No	75%
11AD.09L1System.2	No	Yes	Yes	No	No	75%
11AD.07L2System.4	Yes	No	**No**	No	No	75%
11AE.07L2System.4	Yes	No	**No**	No	Yes	50%
11AF.07L1System.4	Yes	No	**No**	No	Yes	50%
Control Reference 09L1 Average used for CAP Calculation						**68.8%**
Control Reference 07L2 Average used for Gap Calculation						**58.3%**

ai2 assessment:

The following diagram illustrates the processs for identifying CAPs and Gaps in the ai2 assessment:



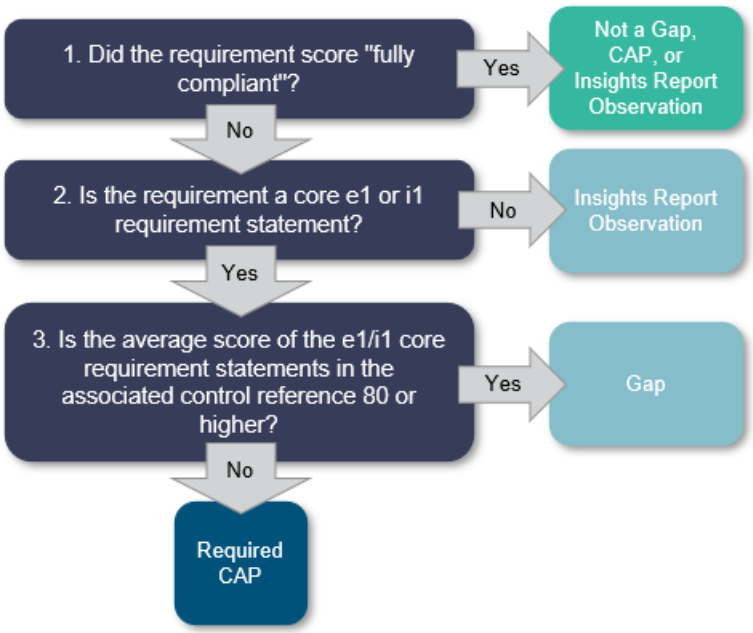
Example of an ai2 assessment with a CAP and Gap:

Requirement Statement	Mapped to ai2 Assessment	Score included in Control Reference Average for CAP Calculation	CAP	Gap	Requirement Statement Scoring
11AA.09AI1System.2	Yes	Yes	Yes	No	50%
11AB.09AI1System.2	Yes	Yes	No	No	75%
11AC.09AI1System.2	Yes	Yes	No	No	75%
11AD.07AI1System.4	Yes	Yes	No	No	75%
11AE.07AI1System.4	Yes	Yes	No	Yes	65%
11AF.07AI1System.4	Yes	Yes	No	No	75%
Control Reference 09AI Average used for CAP Calculation					**66.7%**
Control Reference 07AI Average used for Gap Calculation					**71.7%**

How are CAPs and Gaps calculated for the ai1 assessment when performed in conjunction with an e1 or i1 assessment?

e1 and i1 assessment:

The following diagram illustrates the process for identifying CAPs and Gaps in an e1 or i1 assessment.

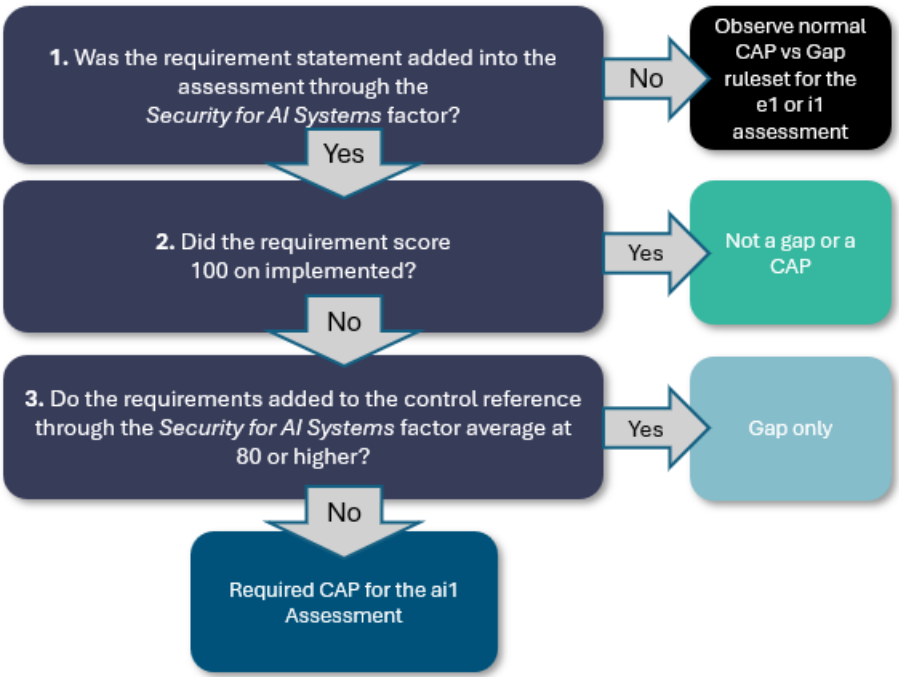


Example of an e1 or i1 assessment with a CAP and Gap:

Requirement Statement	Core e1 or i1 Requirement Statement	CAP	Gap	Requirement Statement Scoring
11AA.09L1System.2	Yes	Yes	No	25%
11AB.09L1System.2	Yes	No	No	100%
11AC.09L1System.2	Yes	No	No	100%
11AD.07L2System.4	Yes	No	No	100%
11AE.07L2System.4	Yes	No	Yes	75%
11AF.07L1System.4	Yes	No	Yes	75%
Control Reference 09L1 Average used for CAP Calculation				**75.0%**
Control Reference 07L2 Average used for Gap Calculation				**83.3%**

ai1 assessment:

The following diagram illustrates the process for identifying CAPs and Gaps in the ai1 assessment:



Example of an ai1 assessment with a CAP and Gap:

Requirement Statement	Mapped to ai1 Assessment	Score included in Control Reference Average for CAP Calculation	CAP	Gap	Requirement Statement Scoring
11AA.09AI1System.2	Yes	Yes	No	No	100%
11AB.09AI1System.2	Yes	Yes	Yes	No	25%
11AC.09AI1System.2	Yes	Yes	No	No	100%
11AD.07AI1System.4	Yes	Yes	No	Yes	75%
11AE.07AI1System.4	Yes	Yes	No	No	100%
Control Reference 09AI Average used for CAP Calculation					75.0%
Control Reference 07AI Average used for Gap Calculation					87.5%

Workflow

Will there be any changes to the existing e1, i1 or r2 assessment workflow?
No.

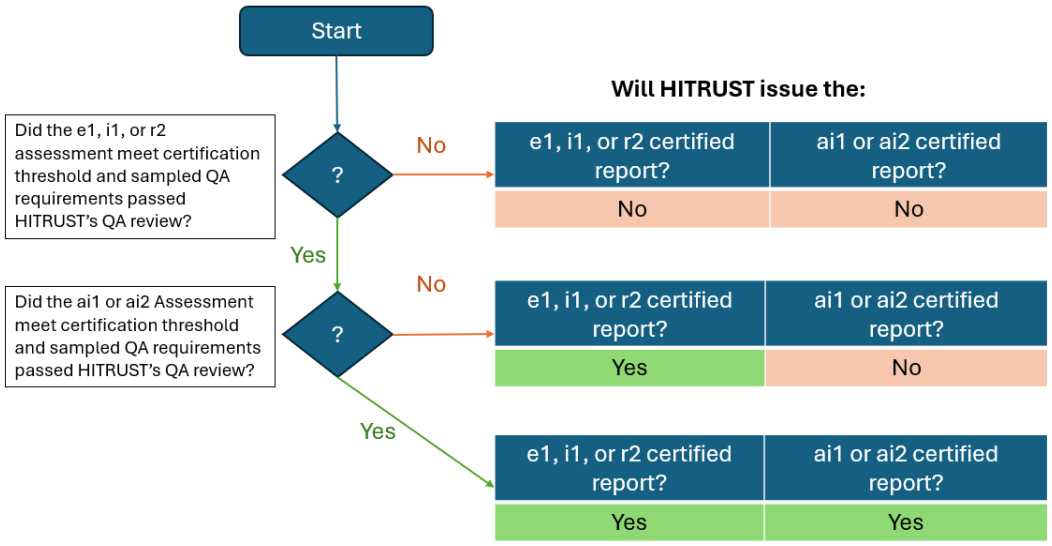
Which assessment types will have the *Assessment Results Review* page available when HITRUST AI Security assessment is included?
e1 and i1 combined assessments.

HITRUST Quality Assurance (QA)

Will HITRUST perform additional QA reviews and/or procedures on the ai1 or ai2 assessment?
Yes, HITRUST will select a sample of requirement statements from those added for the ai1 or ai2 assessment and perform QA procedures.

If the e1, i1, or r2 assessment that the ai1 or ai2 is attached to does not achieve certification (either because it failed HITRUST's QA review or because it did not achieve the control maturity scores needed to certify), will HITRUST still issue the ai1 or ai2 certification?
No. This aligns with our viewpoint that reliable AI security assurances cannot be achieved without accompanying security assurances over the foundational IT systems enabling the delivery of AI capabilities.

When the e1, i1, or r2 certification threshold is achieved, what reports will HITRUST issue if the ai1 or ai2 failed HITRUST's QA review?



For r2 assessments, will HITRUST issue an interim letter for the ai2 assessment when the underlying r2 assessment failed QA review during the interim assessment?
No.

For r2 assessments, will HITRUST issue an interim letter for the underlying r2 assessment when the associated ai2 assessment failed QA review during interim assessment?
Yes.

Can I perform an interim assessment for only the underlying r2 assessment and not the ai2 assessment?
No. The ai2 interim assessment is included as part of the r2 interim assessment and cannot be opted out during interim year.

For r2 assessments, how many interim letters will I receive after satisfying QA review for both the r2 and ai2 assessments?
Two. One for the r2 assessment and one for ai2 assessment.

Reporting

Will there be any changes to the e1, i1 or r2 reports if I add the ai1 or ai2 assessment?
Minimal. In assessments using v11.4.0 and later, assessed entities will be asked to indicate which, if any, in-scope platforms feature AI capabilities (i.e., incorporate an AI model). If the assessed entity is performing an ai1 or ai2 assessment at least one platform must be marked as featuring AI capabilities. Only platforms marked as featuring AI capabilities will be included in the scope of the ai1 or ai2 assessment.

How long is the ai1 or ai2 certification valid?
The ai1 or ai2 certification is valid for the same period as the underlying e1, i1, or r2 certification.

- e1 or i1 certifications combined with an ai1 certification are valid for one year.
- r2 certifications combined with an ai2 certification are valid for two years upon successful completion of an interim assessment by the one-year anniversary of the certification.