



Letter of HITRUST Essentials, 1-year (e1) Certification

November 6, 2025

GBS Corp
7233 Freedom Avenue NW
North Canton, OH 44720-7123 USA

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Essentials, 1-year (e1) Certified for a defined assessment scope. GBS Corp ("the Organization") has chosen to perform a HITRUST CSF v11.4.1 e1 validated assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

Scope

The following platforms of the Organization were included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platform:

- GBS Solutions residing at Ark Data Centers

Facilities:

- Ark Data Centers (Data Center) managed by Ark Data Centers located in Akron, Ohio, United States of America
- Corp HQ - GBS Corp (Office) located in North Canton, Ohio, United States of America
- ITech - GBS Corp (Office) located in Youngstown, Ohio, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST e1 validated assessment report with certification ("Certification") for the Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.



The Certification for the Scope is valid for a period of one year from the date of this letter assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST e1 certification criteria specified as part of the HITRUST Assurance Program.

Users of this letter can contact HITRUST customer support (support@hitrustalliance.net) for questions on using this letter.

The Organization's Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.
- The Organization has implemented the information protection controls as described within their assessment.
- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.
- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.
- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.
- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.
- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.



- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. In HITRUST e1 validated assessments the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.
- Performing sufficient procedures to validate the control maturity scores provided by the Organization.
- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor. HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website (<https://hitrustalliance.net>).

Limitations of Assurance

The HITRUST Assurance Program is intended to gather and report information in an efficient and effective manner. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.



6175 Main Street
Suite 400
Frisco, TX 75034

View this assessment in the
HITRUST Report Center



HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment



Assessment Context

About the HITRUST e1 Assessment and Certification

HITRUST e1 assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving an e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focus on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices () for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals).

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

Assessment Approach

An [Authorized HITRUST External Assessor Organization](#) (the "External Assessor") performed validation procedures to test the implementation and operation of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF



requirements included in the assessment was evaluated by the external assessor in reaching an implementation score.

HITRUST developed a scoring rubric that is used by External Assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- The HITRUST CSF requirement's implementation strength is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the assessment.
- The HITRUST CSF requirement's implementation coverage is evaluated using a 5-point scale (very low through very high) by considering the percentage of the requirement's evaluative elements implemented and operating within the scope of the assessment.

The implementation scoring model utilized on e1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's implementation score.

Implementation Score	Description	Points Awarded
Not compliant- (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat compliant (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75



Implementation Score	Description	Points Awarded
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100



Scope of the Assessment

Company Background

GBS is a 50+ year ESOP Corporation consisting of different divisions, made up of verticals that include services, manufacturing and warehousing. iTECH, is a division of GBS consisting of vertical areas offering technology and services to various facets of the Healthcare industry, including but not limited to Ambulatory Care, Acute Care, Behavioral Health, Specialty Care, Preventative Care and Telehealth/Telemedicine. iTECH services provided include but may not be limited to:

- a) Value Added Reseller (VAR) of NextGen Healthcare Electronic Health Records (EHR) and Practice Management (PM) software: Includes Product sales, Turn-key Implementation services, consulting, custom application development and maintenance support;
- b) Original Equipment Manufacturer (OEM) of EasyID® a Client/Server print management and healthcare digital front door solution: Includes Direct sales, Turn-key Implementation services, consulting, application development and maintenance support;
- c) Document Management Services: Includes scanning, indexing, digital archiving and warehousing of medical records and medical related materials.
- d) Managed Technical Services: Includes the resale and support of data warehousing for the purpose of hosting medical and other affiliated solutions such as Electronic Health Record and Practice Management Software; and
- e) Consumable Sales: Includes the warehousing and sales of consumable materials (paper, labels and wristbands).

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

GBS Solutions	
Description	GBS operates and hosts 1st and 3rd Party solutions within the Ark Data Center, and they consist of but are not necessarily limited to Healthcare related applications including EHR and Practice Management. The hosted environments can, where applicable, provide connections to API's and health data interfaces to facilitate the processing of Protected Health Information (PHI). Secure access to Client hosted applications is performed via VPN connection.



GBS Solutions	
Application(s)	Domain Control, ERP
Database Type(s)	Progress, SQL
Operating System(s)	Windows, AIX
Residing Facilities	Ark Data Centers
Exclusions	AIX ERP (Progress/SQL) not in Scope - this business unit uses NetSuite

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Corp HQ - GBS Corp	Office	No	-	North Canton	Ohio	United States of America
ITech - GBS Corp	Office	No	-	Youngstown	Ohio	United States of America
Ark Data Centers	Data Center	Yes	Ark Data Centers	Akron	Ohio	United States of America



Services Outsourced

The following table presents the outsourced service relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the External Assessor, and
- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Ark Data Centers	Ark is a third-party, HITRUST CSF and SOC-2 certified Data Center providing virtual hardware, networking infrastructure and security primarily for the hosting of GBS Solutions. The hosted environments can, where applicable, provide connections to API's and health data interfaces to facilitate the processing of Protected Health Information (PHI). GBS additionally leverages Ark to provide Backup as a Service and Disaster Recovery as a Service for its own internal corporate infrastructure.	Included