



**A Global Healthcare Technology Company Achieved
HITRUST r2 Recertification Across 3,000+ Healthcare
Automation Systems**

01 Customer Snapshot

Industry	Healthcare Technology
Headquarters	Buchs, Switzerland
Technology Footprint	3,000+ healthcare automation systems worldwide
Certification	HITRUST r2
Additional Framework	HIPAA
Engagement Window	14 weeks
Control Requirements	400+ HITRUST requirements
Assessment Complexity	Expanded scope including new personnel, processes, technologies and Pneumatic Tube Systems infrastructure
Outcome	Successful HITRUST r2 recertification

02 Executive Summary

For a global healthcare technology company operating more than 3,000 healthcare automation systems, HITRUST certification represents a compliance milestone. It provides assurance that the organization's security, privacy, risk-management, and governance practices can withstand formal assessment across a complex technology environment.

The organization was approaching the expiration of its existing HITRUST r2 certification when the scope of its next assessment expanded to include additional personnel, processes, technologies, and infrastructure associated with Pneumatic Tube Systems (PTS). That created a compressed certification challenge.

The organization had 14 weeks to prepare for assessment while addressing 400+ HITRUST control requirements, incorporating an expanded technology environment, aligning applicable requirements with HIPAA, validating evidence, and driving remediation.

Ampcus Cyber established a structured HITRUST readiness and remediation programme covering scope definition, control assessment, evidence validation, risk assessment, remediation, governance, internal audit, and validated assessment preparation.

The engagement culminated in successful HITRUST r2 recertification, while establishing stronger processes for evidence management, risk treatment, governance, and continued compliance readiness.

03 About the Customer



The customer is a global healthcare technology company headquartered in Buchs, Switzerland, providing automation and supply-chain solutions for hospitals and pharmacies.

Its technology footprint extends across 3,000+ healthcare automation systems deployed in medical centers worldwide.

This operating environment makes cybersecurity assurance particularly important. Healthcare technology providers must consider security and privacy requirements alongside the operational realities of technologies deployed within healthcare facilities.

The organization's HITRUST programme therefore needed to reflect not only its corporate security environment but also changes to the technologies, processes, personnel, and infrastructure included in its assessment scope.

04 The Challenge: 14 Weeks to Prepare an Expanded Environment



The organization had previously achieved HITRUST r2 certification. As its certification approached expiration, the next assessment introduced a significant change: the environment being assessed had expanded. Additional personnel, processes, technologies, and infrastructure associated with Pneumatic Tube Systems needed to be incorporated into the programme.

At the same time, the organization needed to address applicable HIPAA requirements alongside HITRUST. The challenge was therefore not simply to repeat a previous certification exercise.

The organization needed to establish, within a fixed 14-week window:

- What had changed since the previous assessment?
- What was now within the assessment boundary?
- Which HITRUST requirements applied to the expanded environment?
- Whether controls remained appropriately implemented?
- Whether evidence could demonstrate control effectiveness?
- Which gaps required remediation?
- How remediation would be tracked?
- How would the organization demonstrate readiness for validated assessment?

With 400+ HITRUST control requirements to address, the programme required more than document collection. It required coordination between scope, controls, evidence, risk, remediation, and governance.

05 Why the Expanded Scope Mattered

The addition of PTS infrastructure changed the assessment context. Pneumatic Tube Systems are deployed within healthcare facilities to support the movement of materials across clinical environments. Bringing associated infrastructure into a security and compliance assessment means the assessment boundary must account for technology that operates within a healthcare setting rather than treating the environment as a conventional corporate IT estate.

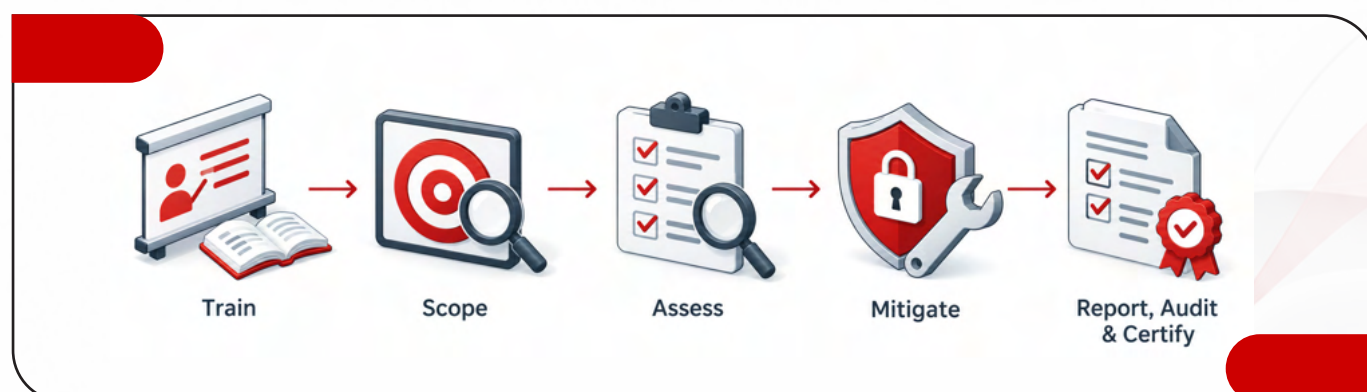
The source material confirms that the organization specifically requested assessment of the infrastructure and environment associated with its Pneumatic Tube Systems. For the HITRUST programme, this meant that scope definition became a critical activity. The organization needed to understand how the newly included environment related to:



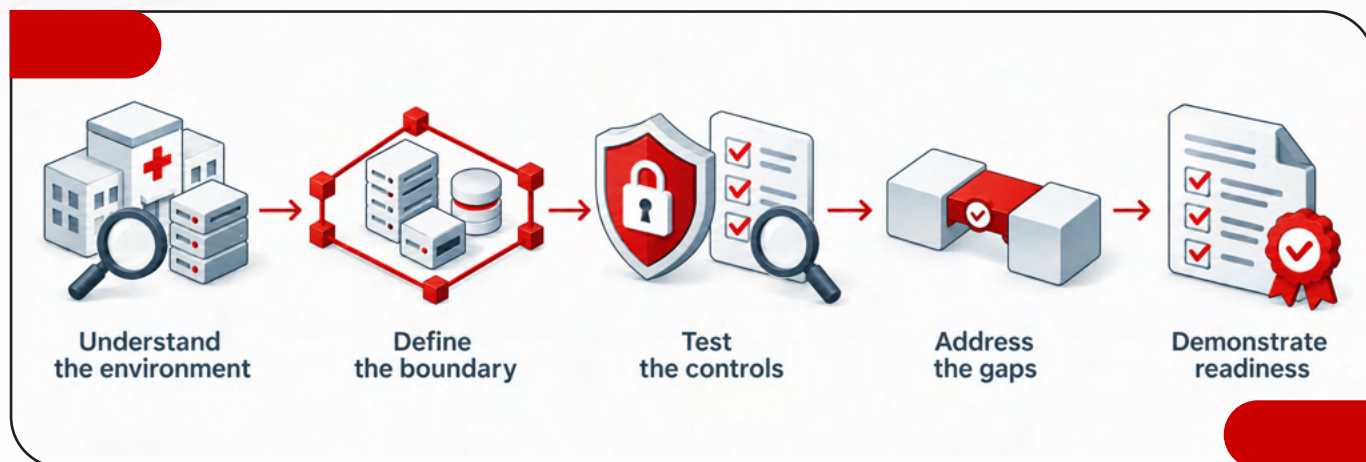
The engagement therefore had to bridge the requirements of a formal healthcare compliance assessment with the operational complexity of an expanding technology environment.

06 The Ampcus Cyber Approach

Ampcus Cyber structured the engagement through a five-stage compliance lifecycle:



Rather than presenting these as isolated consulting activities, the programme connected each stage to the next:



This created a continuous path from preparation to certification.

1. Establishing Governance Before Assessment

The priority was ensuring that the organization had the appropriate stakeholder alignment and governance structure to manage the programme.

Ampcus Cyber:

-  Conducted the project kickoff.
-  Identified key stakeholders.
-  Delivered HITRUST and HIPAA control training.
-  Established an Information Security Management Forum (ISMF).
-  Established an Information Security Task Force (ISTF).

These structures created defined forums for managing security and compliance activities throughout the engagement.

This was important because the assessment involved more than a single security team. Scope definition, evidence collection, remediation, risk treatment, policy updates, and management review required coordinated participation across stakeholders.

2. Defining the Expanded Assessment Boundary

With the environment changing, scope definition became one of the most important technical and governance activities.

Ampcus Cyber worked with stakeholders to understand:

- Business operations
- Data flows
- Critical information
- Assets
- Technologies
- Processes
- Newly included environments
- PTS-related infrastructure
- Project dependencies and risks

The team developed the ISMS Scope Document and Statement of Applicability, while establishing project timelines, dependencies, and risks. This created the documented foundation for determining what needed to be assessed and which requirements applied.

For a risk-based framework such as HITRUST r2, establishing the correct assessment boundary is particularly important because the applicable requirements are determined in the context of the organization's environment and risk factors.

3. Assessing 400+ HITRUST Control Requirements

Once the scope was established, Ampcus Cyber conducted the HITRUST and HIPAA readiness and gap assessment.

The assessment included:

- | | |
|------------------------------------|-------------------------------|
| ■ Control testing | ■ Risk assessment |
| ■ Evidence review | ■ Risk treatment planning |
| ■ Sampling | ■ Policy and procedure review |
| ■ Control-effectiveness evaluation | ■ Evidence preparation |
| ■ Asset identification | ■ HITRUST MyCSF activities |

The programme addressed 400+ HITRUST control requirements across the expanded environment. The focus was not simply on whether documentation existed. The assessment examined whether the organization could demonstrate that applicable controls were implemented and supported by appropriate evidence.

4. Connecting Controls to Evidence

Evidence readiness was a critical component of the engagement. Ampcus Cyber reviewed and supported preparation of:

-  Policies
-  Procedures
-  Supporting documentation
-  Control evidence
-  Assessment artifacts

The team also supported evidence preparation and upload through the HITRUST MyCSF environment. This created a structured relationship between:



That structure helped the organization prepare for the requirements of a validated assessment while reducing the risk of treating evidence collection as a last-minute exercise.

5. Turning Findings Into Remediation

The assessment was designed to produce action, not simply observations. Ampcus Cyber developed a Gap Assessment Report and Action Tracker to identify gaps and mitigation recommendations.

The remediation programme included:

- ▣ Prioritizing control implementation.
- ▣ Tracking remediation activities.
- ▣ Updating policies and procedures.
- ▣ Updating supporting documentation.
- ▣ Revising the Statement of Applicability.
- ▣ Addressing identified non-conformities.
- ▣ Strengthening risk-treatment activities.
- ▣ Conducting internal audits.
- ▣ Facilitating management review.

Bi-weekly compliance meetings provided an operating cadence for reviewing progress, resolving issues, and maintaining accountability. This connected assessment findings directly to remediation rather than leaving the organization with a static gap report.

6. Integrating Risk Management With Compliance

The engagement also incorporated risk-management activities across the programme.

The work included:



This was important because compliance requirements needed to be considered in the context of the organization's actual technology and operational environment.

Rather than treating HITRUST as an isolated certification checklist, the programme connected control requirements with the organization's broader risk-management activities.

7. Preparing for the Validated Assessment

As the programme progressed, Ampcus Cyber supported the organization in moving from readiness activities toward formal assessment.

Activities included:

- HITRUST r2 assessment preparation.
- HIPAA audit support.
- Control-effectiveness review.
- Evidence mapping.
- Sampling preparation.
- Internal quality assurance.
- Assessment preparation and submission.

The organization was therefore entering the validated assessment with scope, evidence, remediation, governance, and control assessment activities already organized.



07 Results

The engagement delivered measurable outcomes across scale, timing, scope, governance, and certification.



- **14-week certification programme:** The engagement was completed within a 14-week window, supporting the organization's certification timeline.
- **400+ HITRUST control requirements addressed:** The programme addressed 400+ HITRUST control requirements across the assessment environment.
- **3,000+ healthcare automation systems:** The customer operates more than 3,000 healthcare automation systems worldwide, providing the scale and operational context for the engagement.
- **Expanded assessment scope:** The programme incorporated additional personnel, processes, technologies, and PTS infrastructure that had not been included in the previous assessment.
- **HITRUST r2 recertification:** The engagement resulted in the organization's successful HITRUST r2 recertification.

08 Business Impact

The value of the engagement extended beyond obtaining a certification.

For a healthcare technology organization operating across thousands of automation systems, maintaining a structured security and compliance programme supports the organization's ability to demonstrate assurance to customers, partners, assessors, and other stakeholders.

Certification continuity

The 14-week programme enabled the organization to progress through an expanded assessment programme within its certification timeline.

Assurance across an expanded environment

The organization incorporated new personnel, processes, technologies, and PTS infrastructure into its assessment activities rather than relying solely on its previous certification scope.

Better connection between compliance and risk

Asset identification, risk assessment, treatment planning, remediation, internal audit, and management review were incorporated into the programme.

More structured evidence management

Control requirements, evidence, testing, findings, and remediation were brought into a more organized assessment workflow.

Stronger governance foundation

ISMS, ISMF, and ISTF structures provided mechanisms for continuing security and compliance oversight beyond the immediate certification exercise.

Readiness for ongoing compliance

The engagement established practices that can support future assessment and certification activities rather than treating HITRUST readiness as a one-time event.

09 Conclusion

The organization began with an approaching HITRUST r2 certification expiration and a significantly expanded environment to assess.

Its next assessment needed to account for additional personnel, processes, technologies, and Pneumatic Tube Systems infrastructure, while addressing 400+ HITRUST control requirements within a 14-week engagement window.

Ampcus Cyber brought these requirements together through a structured readiness and remediation programme covering scope definition, control assessment, evidence validation, risk management, remediation, governance, internal audit, and validated assessment preparation.

The result was successful HITRUST r2 recertification, alongside strengthened processes for evidence management, risk treatment, governance, and continued compliance readiness.

For healthcare technology companies, HITRUST readiness is not merely an audit exercise. It is an opportunity to establish a repeatable connection between technology, security controls, risk, evidence, remediation, and organizational assurance.



Prepare for Your HITRUST Assessment with **Ampcus Cyber**

Get expert support to assess your environment, close control gaps, strengthen evidence readiness, and approach certification with confidence.