Pre-Conference Workshop

HITRUST Scoping Exercise
Introduction

Track: Pre-Conference
Date | Room: Monday, May 20 | Texas 1-2
Time: 10:30 – 11:30 AM
Speakers: Michael Frederick, HITRUST
          Eric Moriak, HITRUST
          Jeremy Huval, HITRUST
Agenda

This session is designed to provide a couple of examples of scoping an assessment using the HTIRUST CSF, the MyCSF Tool and the assurance process. HITRUST’s scoring methodology used during the assessment process. It will also focus on expected sampling methodology for requirement statement testing. Topics will include:

Scoping Fundamentals
• What does HITRUST certify
• Who sets the Scope
• Carve outs of scope
• Assessment Objects
• What and Why Am I Doing This
• An Assessment Object Versus the Elements within Scope

Scoping Examples
• Example #1 (Consulting Firm)
• Example #2 (A SaaS Provider)
Scoping Fundamentals
Scoping Fundamentals
What does HITRUST Certify?

HITRUST only certifies implemented systems.

- HITRUST does **not** certify facilities, people, services or product. It must be an implemented environment for a certification to be awarded.

Example: HITRUST cannot certify a vendor’s products which have not been implemented.
Scoping Fundamentals
What does HITRUST Certify?

Further, HITRUST does not certify organizations, only those implemented systems that have undergone a validated assessment.

Although an organization may include all of their systems within the scope of an assessment, new systems may be added after the point that a certification was issued and these new systems would not be included/grandfathered into the original scope.

When relying on another entity’s certification, always ensure that the defined scope of that assessment was commensurate with your organization’s need.
Scoping Fundamentals
Who sets the Scope

- The scope of an assessment determines the boundary for what will be reviewed in the assessment. However, the scope must be defined with a clear logical or physical boundary.
- Client management defines the scope of the assessment
- The scope of the assessment should consider the organizational business, related systems, facilities, service providers, etc.
- Ensures that the necessary data is collected in an effective and efficient manner
- The tool and the process are designed to be flexible and adaptive so that it can be tailored to fit the unique environment of an organization based upon size and complexity

Note: By clearly defining and identifying upfront the scope of the HITRUST CSF assessment at the organization, the entity will focus and streamline analysis and information gathering tasks resulting in a timely completion of the assessment with a detailed report
Scoping Fundamentals
Carve Outs

In general, HITRUST does not allow for “carve-outs” when setting the scope for an assessment.

For example, when an organization is seeking certification over one of their implemented applications and that application supports multiple business functions, then the entire application with all of its business functions should be within scope.
Scoping Fundamentals
Carve Outs

If there are carve outs in the scope of the assessment, these exclusions will be identified in the scope of the certification letter/report.

The certification letter/report may list that which was in scope, as well as listing those areas that were excluded from scope.
Scoping Fundamentals
Assessment Objects

• MyCSF allows organizations to define the scope of their environment.
  • Focus on your need (Internal requirement, external need, support the business, etc.)
• An assessment object is what the organization is attempting to certify within their validated assessment. It is the entire scope.
• There are also elements within scope. These are the individual items that need to be tested.
• An organization can have a Single (efficient) assessment object or Multiple assessment objects (increased data accuracy)
• For certification, a report is also needed for each assessment object
  • Multiple Assessments = Multiple Reports
Scoping Fundamentals

What and Why Am I Doing This?

• MyCSF allows organizations to define the scope of their environment.
  • Focus on your need (Internal requirement, external need, support the business, etc.)
• An assessment object is what the organization is attempting to certify within their validated assessment. It is the entire scope.
  • There are also elements within scope. These are the individual items that need to be tested. What is the purpose of this assessment/compliance work
    • Internal (Audit) requirements
    • External requirements (Regulatory)
    • Support BA or third-party requirements
    • Demonstrate compliance internally
    • Improve security posture/stance
    • Competitive Advantage
    • Other……

Without this information, scoping is infinitely harder and more complex.
Scoping Fundamentals
An Assessment Object Versus the Elements within Scope

- Scope is defined as the complete target for how the organization intends to use MyCSF and the HITRUST CSF for:
  - Assessments
  - Implementation of controls
  - Remediation tracking

- Your ‘assessment object’ equates to the scope
- The assessment object may include the *entire environment* (e.g., *all implemented systems within your organization*).
- The assessment object may also be *segmented* into portions (i.e., scope elements) of the entire environment, depending on the organization’s particular needs and structure
  - Meaningful use
  - NIST
  - Internal audit requirement
  - Third Party assessment needs
Scoping Fundamentals
An Assessment Object Versus the Elements within Scope

Within a scope, an assessment may include elements such as:

- Business Units
- Facilities
- Departments
- Applications
- Servers and Databases
- Network Infrastructure
- Information Security Control Systems
- Business Associate / Vendor
Scoping Fundamentals
An Assessment Object Versus the Elements within Scope

• An **Element** is each individual item included in a scope
  • A scope can include many elements (i.e. – applications, technologies, etc.)
  • Elements are linked together to define the scope of an assessment

• An **Object** in MyCSF equates to an assessment. It is the scope of the targeted certification. It can include:
  • One or more facilities
  • One or more business units
  • One or more departments
  • One or more applications
  • Other technologies
  • Etc.
Scoping Example #1
Consulting Firm
Scoping Example #1

Scenario

In this scenario, a consulting firm has been asked to obtain HITRUST certification by one of their clients. They want to ensure that controls are in place to protect their environments.

The contract stipulates that they:

– Provide development and monitoring services for their client
– All development work is to be done internally on a consultant’s internally managed infrastructure
– After UAT, approved development is transitioned into the client’s environment
– All monitoring activities are performed within the client’s production environment
Scoping Example #1
Should the following be within scope?

- The consultant’s endpoints?
  Yes, these are the devices the consultants use to connect

- The client’s endpoints?
  No, this would be under the client’s responsibility

- The consultant’s development environment?
  Yes, as all development work is performed here

- The client’s production environment?
  No, this is the responsibility of the client to certify

- The consultant’s internal network?
  Yes, it is across their internal network that they establish the connection

- The client’s internal network?
  No, this is the responsibility of the client to certify
Scoping Example #1
Should the following be within scope?

- The consultant’s VPN services?
  Only if the consultant uses their internal VPN to deliver defined services

- The client’s VPN services?
  No, this is the responsibility of the client to certify

- The consultant’s Active Directory (AD) server?
  Yes, this is where consultant authentication and access controls are managed

- The client’s Active Directory (AD) server?
  No, this is the responsibility of the client to certify
Scoping Example #1
Should the following be within scope?

– The consultant’s vulnerability scans?
  Yes, across their Development, AD and VPN environments

– The consultant’s Business Continuity/Disaster Recovery Plans?
  Yes, as they apply to the environments listed above

– The consultant’s Internal Incident Monitoring?
  Yes, especially if it results in notifications to the customer regarding the in-scope systems

– The consultant’s Risk Management plans?
  Yes, as it applies to the in-scope environment

– The consultant’s Physical Security plans?
  Yes, in regards to the in-scope systems listed above
Scoping Example #1

Summary

The scope of the assessment is defined by the entity seeking certification.

In this example, it should be collaborated on between the consulting firm and the client asking them to become certified.

Note – Although HITRUST may question scope during the processing of an assessment, it is ultimately the assessed entity’s responsibility to define it.
Scoping Example #2
A SaaS Provider
Scoping Example #2

Scenario

In this scenario, a SaaS provider is seeking HITRUST certification for their environments where they host their client’s applications. They want to provide assurances over their model for providing a cloud computing environment for prospective clients.

In this scenario, there are no contracts …

The SaaS provider only wants to certify the infrastructure for the containers where these services are being offered. However, there are multiple clients currently leveraging this offering.
Scoping Example #2
Should the following be within scope?

- The SaaS provider’s endpoints?
  Not required, if the focus is solely the containers, endpoints may not be within the scope of the assessment

- The client’s endpoints?
  No, this would be under the client’s responsibility

- The SaaS provider’s development containers?
  Only if they had included them within the scope of the assessment

- The client production environments running within the containers?
  No, this is the responsibility of the client who owns the applications to certify

- The SaaS provider’s internal network?
  Yes, as it applies to their client’s and client customer’s ability to connect to these environments

- The internal networks of the SaaS provider’s clients and/or their client’s customers?
  No, this is the responsibility of the client to certify
Scoping Example #2
Should the following be within scope?

– The SaaS providers VPN services?
  Only if the cloud provider uses their internal VPN to support these environments

– The VPN services of a client leveraging the SaaS provider?
  No, this is the responsibility of the client to certify

– The SaaS provider’s Active Directory (AD) server?
  Most likely, this is where the cloud provider’s admin’s authentication and access controls are managed

– The Active Directory (AD) server of a client leveraging the SaaS provider?
  No, this is the responsibility of the client to certify
Scoping Example #2
Should the following be within scope?

– The SaaS provider’s vulnerability scans?
  Yes, across the infrastructure supporting these containers

– The SaaS provider’s Business Continuity/Disaster Recovery Plans?
  Yes, as it applies to recovery of the containers only. Hosted software within the containers may or may not be part of a contractual obligation and would likely be outside the scope of this scenario. These are typically managed by the client.

– The SaaS provider’s Internal Incident Monitoring?
  Yes, as it applies to the containers that are within scope

– The SaaS provider’s Risk Management plans?
  Yes, as it applies to the containers that are within scope

– The SaaS provider’s Physical Security plans?
  Yes, as it applies to the containers that are within scope
Scoping Example #2

Summary

The scope of this assessment is defined by the SaaS provider. They are not seeking to certify their client environments for them. They are only seeking to certify the containers into which they host their client’s systems.

In this example, there is no scope coordination with the clients of the provider. It is the clients responsibility to ensure that the certified environment is commensurate with the service delivery that they wish to see certification over.
Open Discussion and Questions
Visit [www.HITRUSTAlliance.net](http://www.HITRUSTAlliance.net) for more information

To view our latest documents, visit the **Content Spotlight**