Crowe Horwath.

Smart decisions. Lasting value.℠

Crowe Healthcare Webinar Series

HITRUST CSF™ Assessment Services

September 27, 2017

HOUSEKEEPING

- All audio for today’s session will be streamed directly to your computer.
- Please submit questions through the Q&A function on your screen.
- To download the presentation, click the resources icon at the lower part of your event console.
- CPE credit
  - Login individually to the session for at least 50 minutes
  - Successfully complete polling questions
- NO CPE credit
  - Fail to successfully complete 3 of 4 polling questions
  - View a recording of this session (CPE is only awarded for live sessions)
- CPE certificate of completion will be e-mailed within two weeks of successfully passing this program

Crowe Horwath.

Smart decisions. Lasting value.™

Crowe Healthcare Webinar Series

HITRUST CSF™ Assessment Services

September 27, 2017

Today's Presenters

Jared Hamilton, CISSP, CCSK, HITRUST Certified CSF Practitioner
Senior Manager
Healthcare Cybersecurity Solutions Leader
+1 317.706.2724
jared.hamilton@crowehorwath.com

Erika Del Giudice, CISA, CRISC, HITRUST Certified CSF Practitioner
Senior Manager
HITRUST Solution Leader
+1 630.575.4366
erika.delgiudice@crowehorwath.com

Matt Gopin
Walgreens Boots Alliance
Vice President, WBA IT Governance, Risk & Compliance
+1 847.964.8195
matt.gopin@wba.com

Agenda

- Growing Healthcare Cybersecurity Risks
- Cybersecurity Frameworks
- HITRUST MyCSF™ Overview
- Adopting HITRUST™
- HITRUST™ Certification
- Client Testimonial
- Questions and Answers

Rising Cybersecurity Risks in Healthcare

“Do more with less”

More to Protect

- Electronic Health Records
- Health Information Transfers
- Mobile Devices & Applications
- Biomedical Devices
- Internet of Things (IoT)

Increased Threats

- Phishing Attacks
- Ransomware
- Lost or Misplaced Data
- Untrusted Vendors

Escalating Regulatory Pressures

- HIPAA
- Meaningful Use / MIPS

Lack of IT Security Professionals

Poll Question #1

What are you most worried about from a cybersecurity risk perspective?

A. An external attack or breach of patient records

B. Medical systems unavailable for patient care

C. Regulatory fines

D. Loss of reputation due to media coverage of an incident

E. Other

Organizing Controls around Frameworks

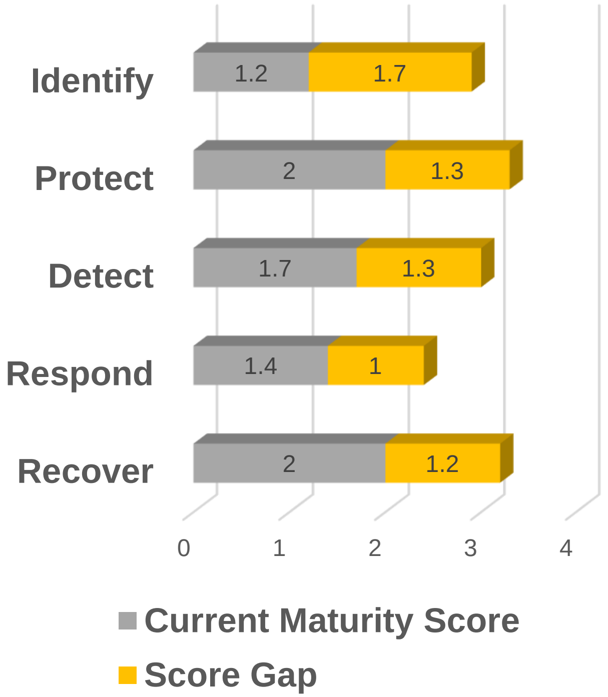
What Frameworks Provide:

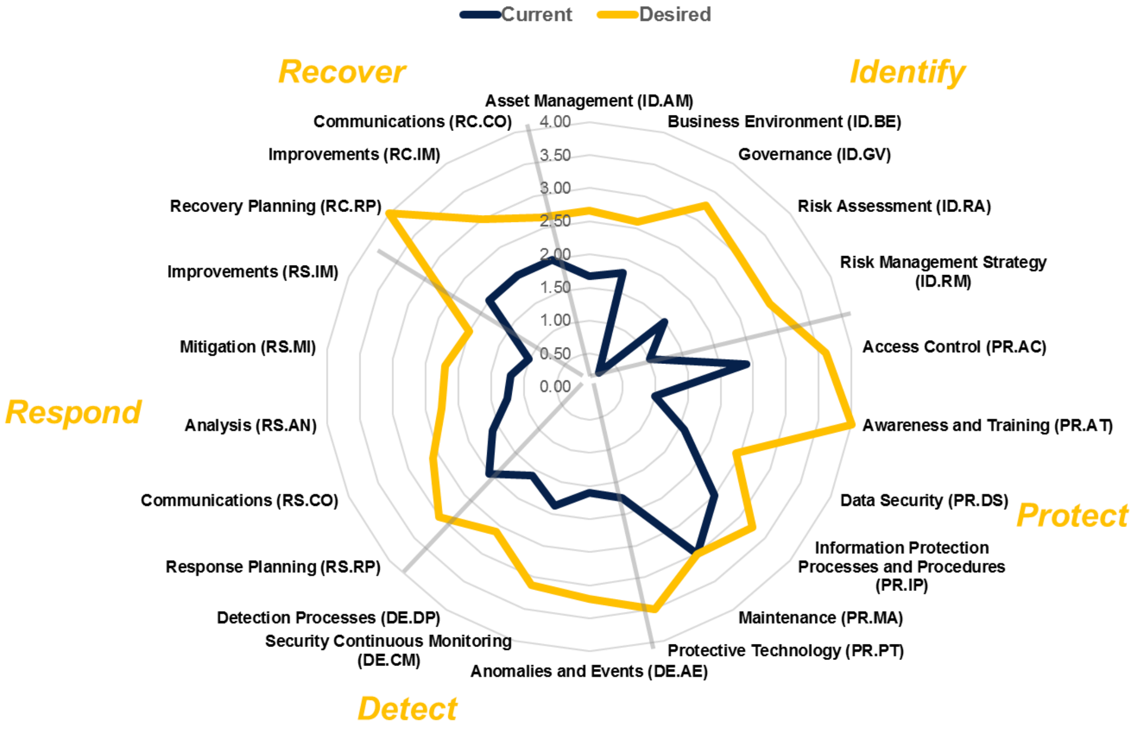
- Align and organize IT Security controls
- Can provide reporting metrics for organizations to apply proper levels of IT security controls

Common IT Control Frameworks:

- ISO 27001
- NIST Cybersecurity Framework (800-53 Controls)
- COBIT
- HITRUST CSF™
- Cloud Security Alliance (CSA)
- Center for Internet Security (CIS)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Crowe Cybersecurity Risk & Control Framework

NIST Cybersecurity Framework Example





NIST CSF Maturity Scale

1 = Partial

2= Risk Informed

3=Repeatable

4=Adaptive

Poll Question #2

Do you currently align with any of these frameworks?

A. ISO 27001

B. NIST Cybersecurity Framework (800-53 Controls)

C. COBIT

D. HITRUST CSF™

E. Cloud Security Alliance (CSA)

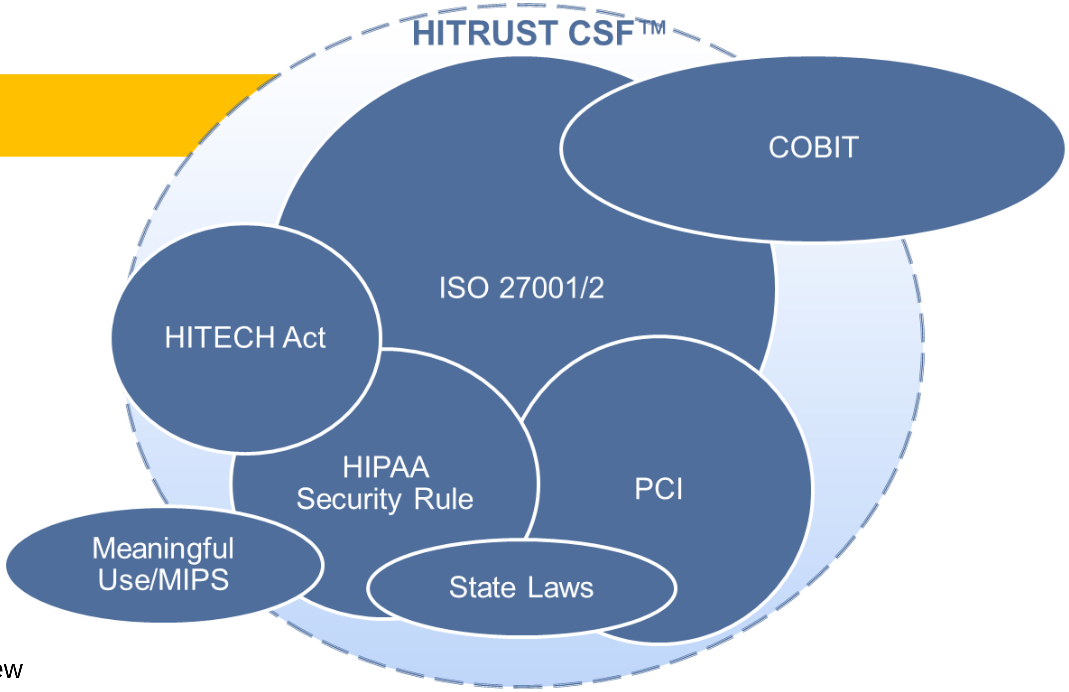
F. Center for Internet Security (CIS)

G. AICPA SOC 2 Trust Services Principles (TSP) Criteria

HITRUST CSF™ Introduction

HITRUST CSF™

- Provides coverage across multiple standards and includes significant components from well-respected IT security standards bodies
- Started with ISO/IEC 27001:2005 and evolved to include:
  - HIPAA/HITECH
  - State Privacy Laws
  - PCI
  - COBIT
  - NIST
  - FTC
  - CMS
  - California Civil Code
  - Texas Medical Privacy Act
  - FFIEC IT Examination (InfoSec)
  - FedRamp
  - Department of Homeland Security (DHS) Resilience Review



Harmonizes existing controls and requirements from standards, regulations, business and third-party requirements

Incorporates both compliance and risk management principles

Defines a process to effectively and efficiently evaluate compliance and security risk, which includes the HIPAA Final Rule Requirements

Supports HITRUST CSF™ Certification

HITRUST CSF™ Components

Control Categories

- Based on ISO 27001 Appendix A
- 14 control categories (13 security, 1 privacy)

Control Objectives

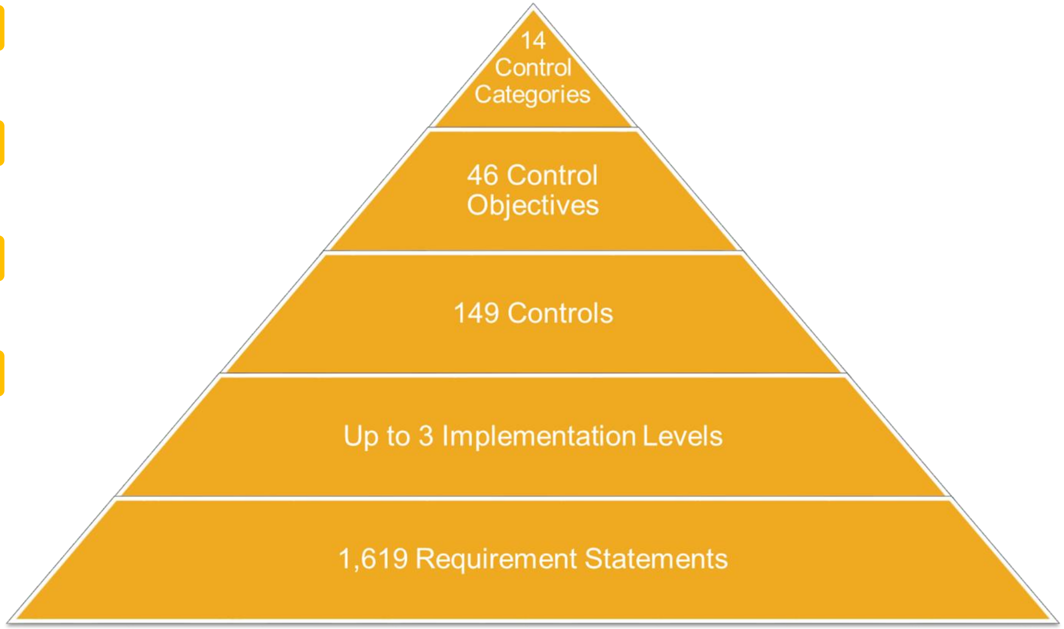
- Desired risk reduction goal
- 46 control objectives

Implementation Requirements

- Prescriptive (required) control statements
- 149 controls

19 Assessment Domains:

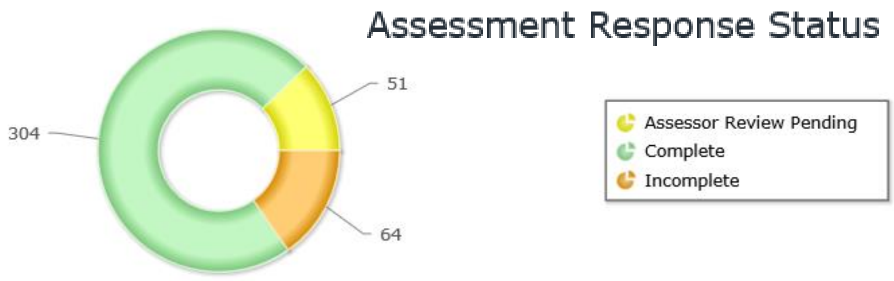
- Information Protection Program
- Endpoint Protection
- Portable Media Security
- Mobile Device Security
- Wireless Security
- Confirmation Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Password management
- Access Control
- Audit Logging & Monitoring
- Education, Training & Awareness
- Third-Party Assurance
- Incident Management
- Business Continuity & Disaster Recovery
- Risk Management
- Physical & Environmental Security
- Data Protection & Privacy

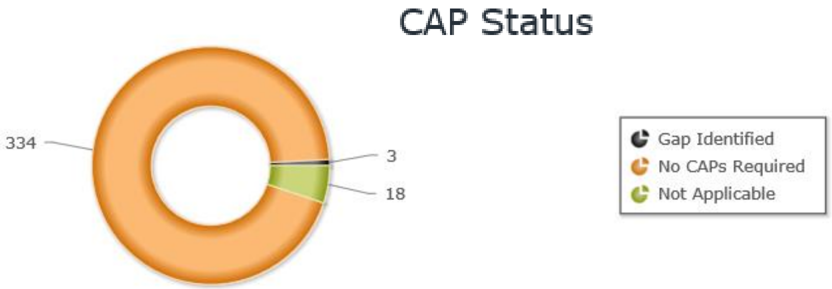


HITRUST™

HITRUST MyCSF™ Tool

- Web Based Portal
  - Build customized control sets based on your organization’s scope
  - Create HITRUST CSF™ Object
  - Perform validation testing
  - Capture correction action plans (CAPs)
  - Manage policies
  - Manage exceptions
  - Receive dashboard reporting
  - Benchmark across similar organizations
  - Requires HITRUST MyCSF™ Subscription





HITRUST CSF™ Assessments

Assessment Options

- Self Assessment
  - Lower degree of testing
  - Provides self-assessment report
- Validated Assessment
  - Requires Approved HITRUST CSF Assessor to validate results
  - Higher degree of testing and trust
  - Provides validated report or validated report with certification (if passing)

Maturity Models

- 1 - Policy
- 2 - Process
- 3 - Implemented
- 4 - Measured
- 5 - Managed

Control Scoring

- Non-Compliant (NC)
- Somewhat Compliant (SC)
- Partially Compliant (PC)
- Mostly Compliant (MC)
- Fully Compliant (FC)

Corrective Action Plans (CAPs)

What if there are issues identified?

- For a certified report, each domain MUST score a 3+ or a 3 with CAPs
- Any domains that do not score at least a 3 will result in the generation of a validated report, not a certification
- Any control implementation requirement that scores less than a 3+ will require a CAP
- You can be certified with CAPs as long as the overall score of all domains is 3

Interim Assessment

At the 1-year anniversary of the Certification, an interim assessment is required to be performed.

Interim assessment MUST be submitted no later than 60 days after the 1-year anniversary date.

Re-Assessment process is as follows:

- Assessed entity must update the scoping questions
- We review the updated questionnaire for changes to original questionnaire
- Test at least 1 control/statement in each domain
- Review the status of any CAPs from the original assessment and ensure satisfactory progress/milestones are being met

Poll Question #3

Do you know where your PII resides?

A. Yes, my organization knows where it’s at and we update our inventory periodically
B. Yes, I am pretty comfortable my organization knows where all PII resides
C. No, my organization doesn’t track where PII is stored
D. No, I have no clue

SOC 2 vs HITRUST CSF™

SOC 2

- Owned by the AICPA
- Provides information on processes and controls at a service organization with a service auditor’s opinion
- For organizations needing to address the controls related to any of the 5 TSP
- Reporting framework
- Uses the TSP Criteria
- Organizations must meet ALL criteria for the selected principles
- Issued by a CPA firm

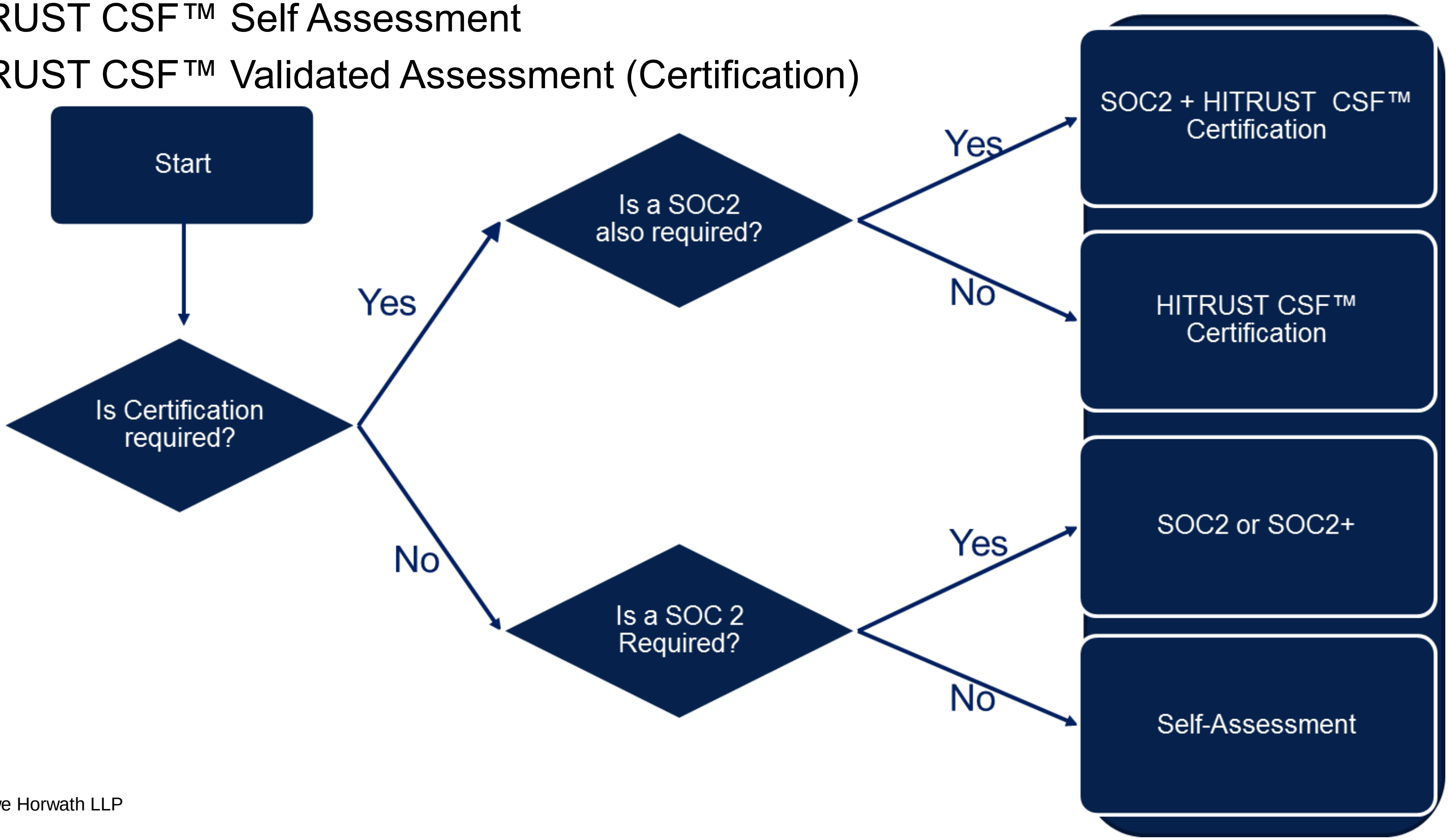
HITRUST CSF™

- Owned by HITRUST™
- Leverages standards and regulations to establish a common security and privacy framework for healthcare organizations, business associates and healthcare information exchanges
- Provide organizations with prescriptive implementation requirements
- For organizations with PHI (create, access, store or process)
- Security framework
- Uses the HITRUST CSF™ Framework
- Implementation requirements are driven by risk factors identified by the organization
- Issued by an Approved HITRUST CSF™ Assessor

HITRUST™ and the AICPA have collaborated to publish guidance including a mapping of the HITRUST CSF™ to the Trust Service Principles (Security, Confidentiality and Availability) along with a reporting template and practitioner guide with FAQs

HITRUST CSF™ Report Options

- SOC 2
- SOC 2+
- SOC 2+ HITRUST CSF™ Certification
- HITRUST CSF™ Self Assessment
- HITRUST CSF™ Validated Assessment (Certification)



Poll Question #4

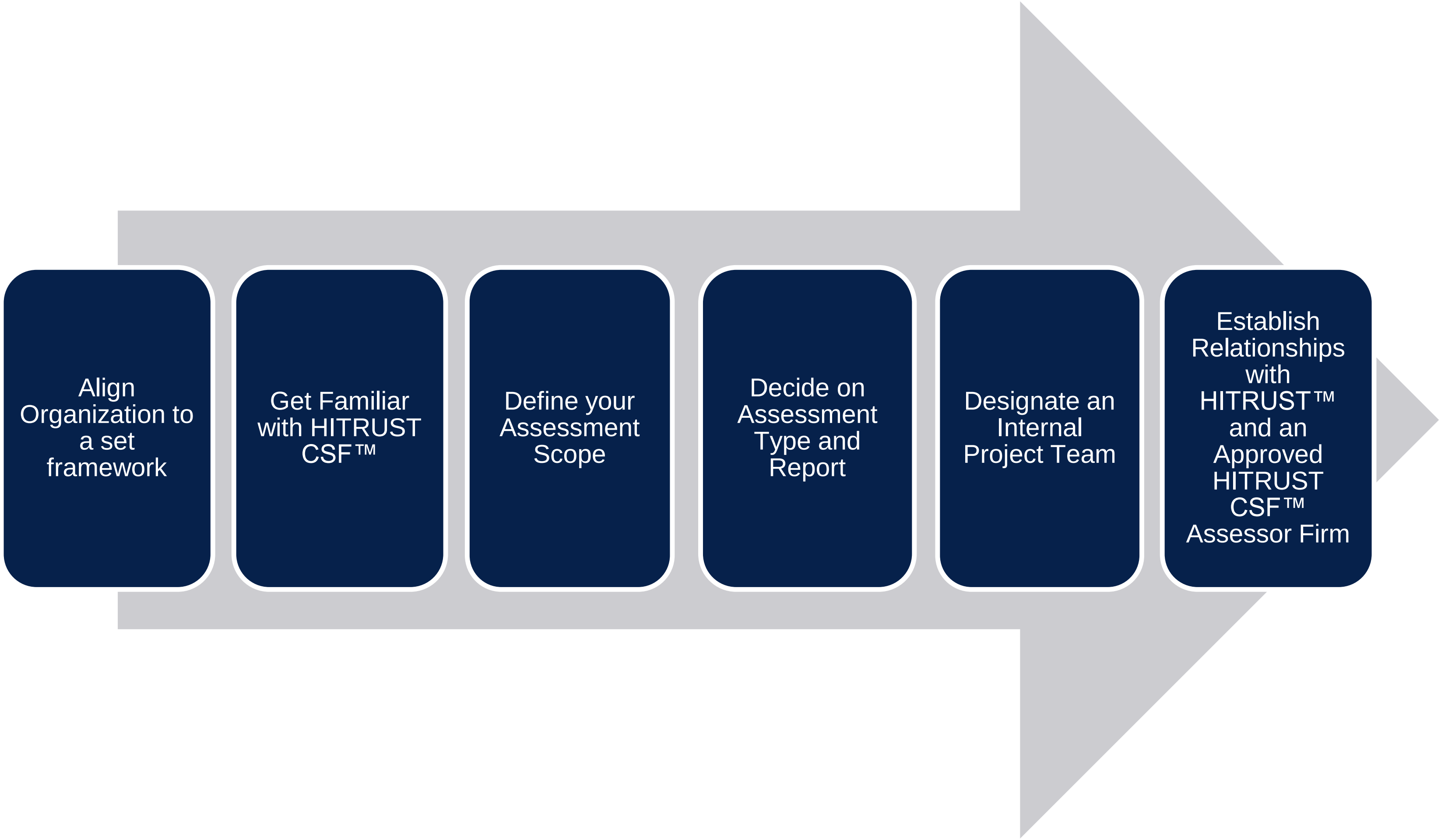
Has your organization used other frameworks in the past and you think HITRUST™ might be more valuable to your organization and it’s customers?

A. Yes, definitely think HITRUST™ would be more valuable than performing several other assessments
B. Yes, I somewhat feel that our customers would value or prefer a HITRUST™ to other frameworks
C. No, I think our current framework assessments are fine
D. No, I’m not sure

A Client’s Perspective

- What drove you to pursue a HITRUST™ Certification?
- Benefits you’ve seen or are hoping to achieve
- Your experience so far with the HITRUST CSF™ framework

How do I get started with HITRUST™?



Align Organization to a set framework

Get Familiar with HITRUST CSF™

Define your Assessment Scope

Decide on Assessment Type and Report

Designate an Internal Project Team

Establish Relationships with HITRUST™ and an Approved HITRUST CSF™ Assessor Firm

Questions

Jared Hamilton
Direct 317.706.2724
Jared.Hamilton@crowehorwath.com

Erika Del Giudice
Direct 630.575.4366
Erika.delgiudice@crowehorwath.com

Matt Gopin
Direct 847.964.8195
Matt.Gopin@wba.com

Cybersecurity Watch Blog

www.crowehorwath.com/cybersecurity-watch