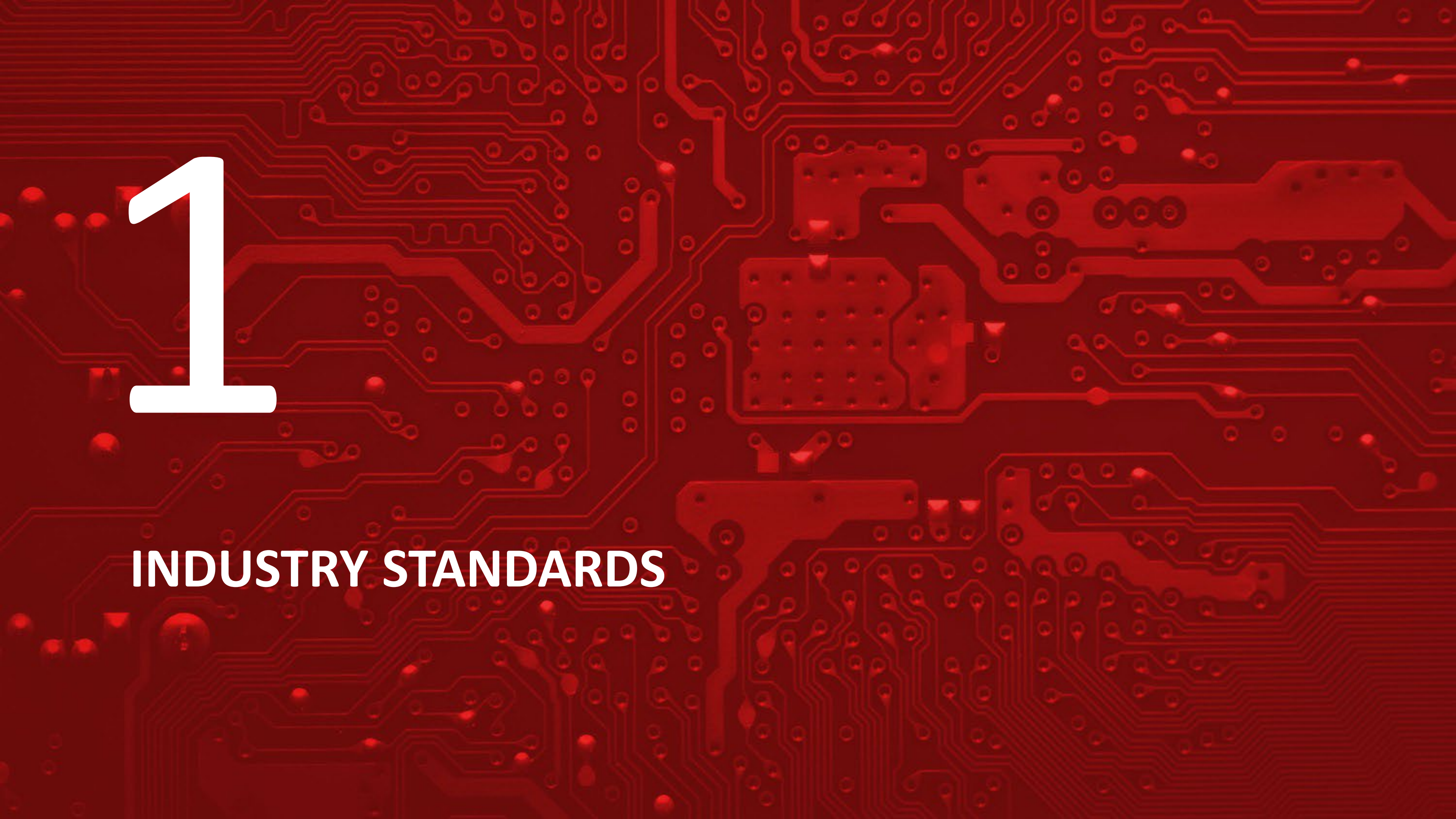
HITRUST as a Standards Organization

Topics

1. Industry Standards
2. Standards Organizations
3. The HITRUST CSF
4. Comparing Organizations
5. Summary/Conclusion
6. About HITRUST



1

INDUSTRY STANDARDS

Industry Standards

What is an industry standard?

- A set of criteria within an industry relating to the standard functioning and carrying out of operations in their respective fields of production (https://definitions.uslegal.com/i/industrial-standards/)
- Generally accepted requirements followed by members of an industry (https://definitions.uslegal.com/i/industrial-standards/)
- An established standard, norm, or requirement in a particular area of business (https://www.collinsdictionary.com/dictionary/english/industry-standard)
- A set of "universal" operational process methods or tools that are applicable to most companies within a specific industry, which identifies the core dimensions, materials and methodologies those companies may use and support business practices (http://smallbusiness.chron.com/definition-industry-standard-model-15638.html)

Industry Standards – Pros & Cons

Benefits

- Established models can provide significant savings to adopting organizations
  - Effort
  - Time
  - Money
- Industry vetting helps reduce problems/loss
- Provides consistency across organizations in the industry

Disadvantages

- Not part of a company's intellectual capital (i.e., no "secret sauce")
- Less support for innovation (i.e., standards based on what's already been done)
- It can take years for a proposed standard to go from initial concept to broad acceptance

(http://smallbusiness.chron.com/definition-industry-standard-model-15638.html)

2

STANDARDS ORGANIZATIONS

Standards Organizations

What is a standards organization?

- **Sometimes referred to as a standards body, standards developing organization (SDO), or standards setting organization (SSO), a standards organization**
  - Provides an orderly and systematic formulation, adoption, or application of requirements (standards) used in a particular industry or sector of the economy (https://definitions.uslegal.com/i/industrial-standards/)
  - Provides requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose (https://www.iso.org/standards.html)
- **It is estimated that in the U.S. today there are hundreds of "traditional" standards developing organizations - with the 20 largest producing 90% of the standards - and hundreds more "non-traditional" standards development bodies, such as consortia (https://www.ansi.org/about_ansi/introduction/introduction?menuid=1)**

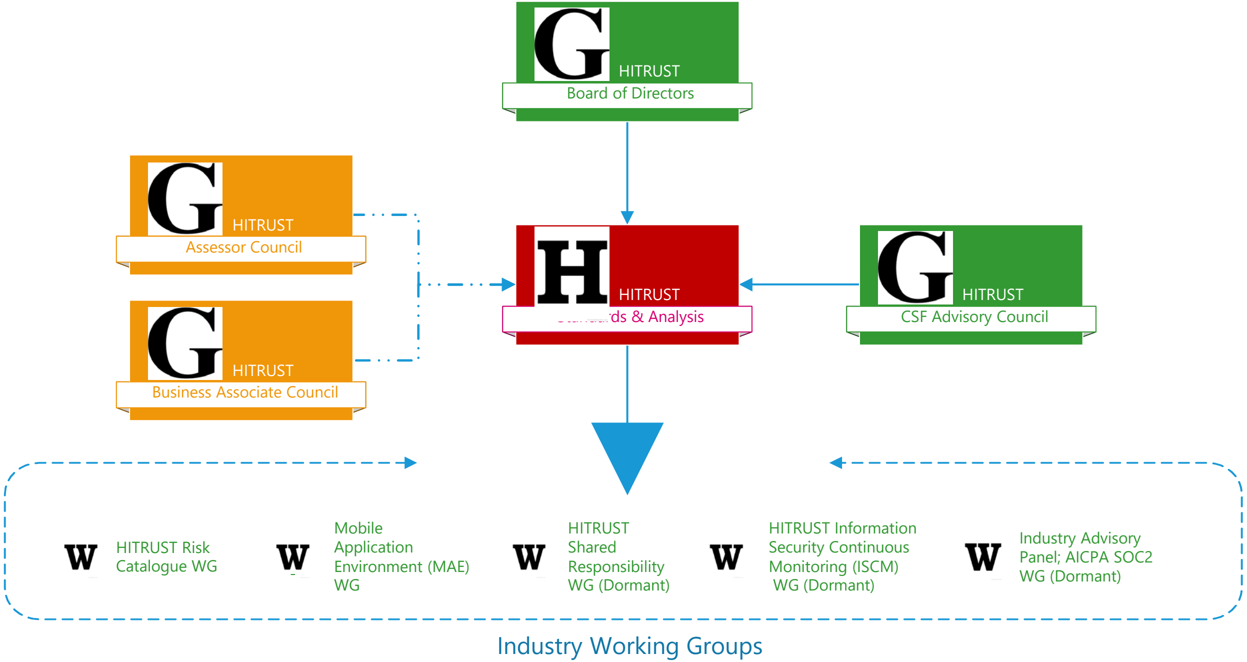
Standards Organizations – Examples

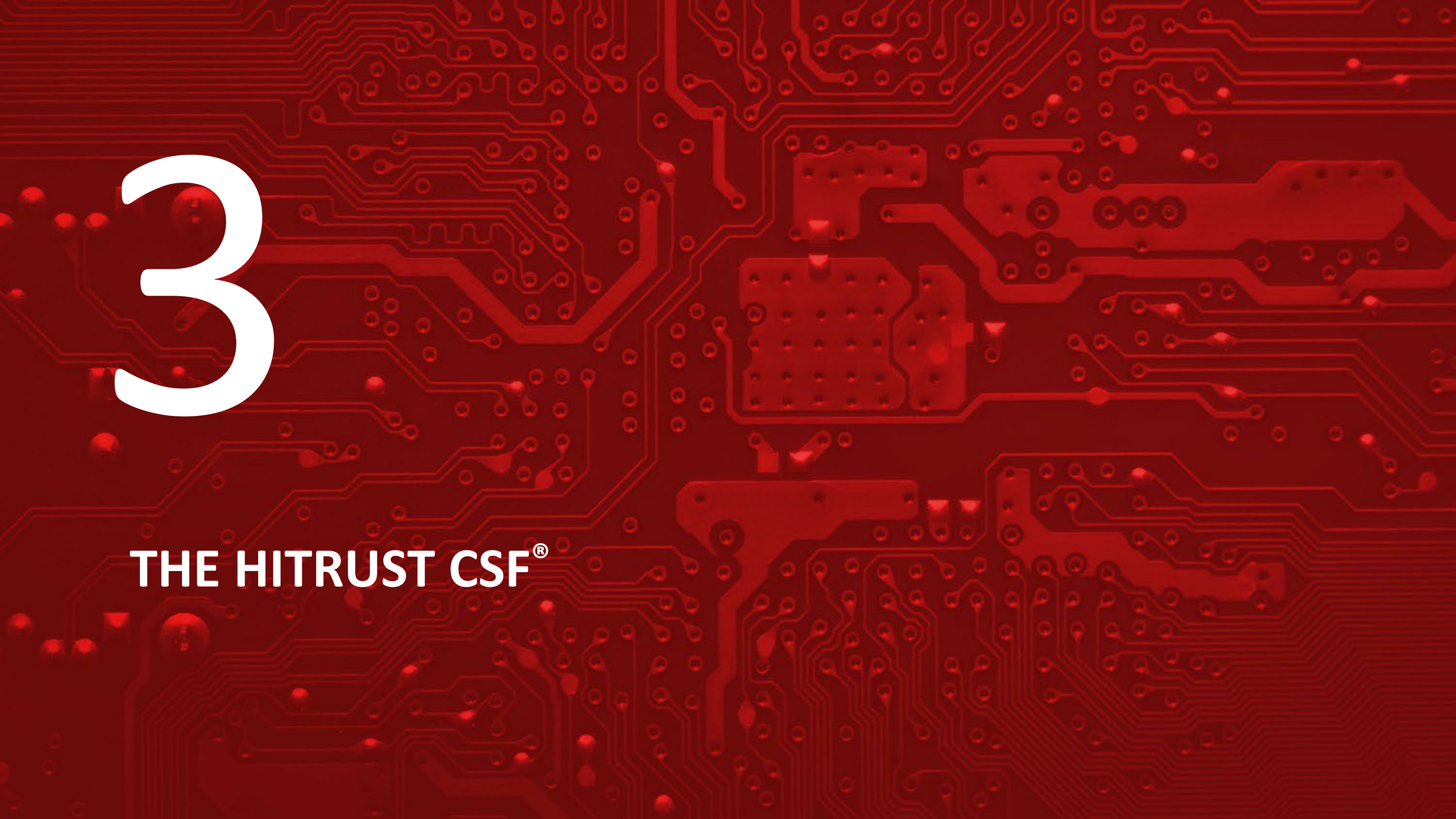
Standards organizations include, but are not limited to:

- ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States
- EHNAC (Electronic Healthcare Network Accreditation Commission) provides standards on transactional quality, operational efficiency and data security in healthcare
- HITRUST® provides an information security and privacy control standard used by a variety of industry sectors
- ISACA (previously Information Systems Audit and Control Association) supports the development, adoption and use of standards and practices for information systems
- ISO (Organization for International Standards) develops and publishes international standards on a wide range of applications, including information security
- NIST (National Institute of Standards & Technology) is a U.S. government organization that provides standards for numerous applications, including computers & information systems
- PCI SCC (Payment Card Industry Security Standards Council) provides security requirements for entities that accept, transmit or store cardholder data

The HITRUST Standards Organization

- The HITRUST standards organization (H) is governed (G) by a Board of Directors and receives industry guidance (G) from multiple industry councils
- The work of the HITRUST standards organization is supported by multiple industry working groups (W), which change from time-to-time based on need


G HITRUST Board of Directors
G HITRUST Assessor Council
G HITRUST Business Associate Council
H HITRUST Standards & Analysis
G HITRUST CSF Advisory Council
W HITRUST Risk Catalogue WG
W Mobile Application Environment (MAE) WG
W HITRUST Shared Responsibility WG (Dormant)
W HITRUST Information Security Continuous Monitoring (ISCM) WG (Dormant)
W Industry Advisory Panel; AICPA SOC2 WG (Dormant)
Industry Working Groups



3

THE HITRUST CSF®

The HITRUST CSF Standard

- Provides coverage across multiple regulations and includes significant components from other well respected IT security standards bodies and governance sources
- Is scalable, risk-based, industry-agnostic and certifiable

Legislative, Regulatory, and ‘Best Practice” Standards and Frameworks include, but are not limited to:

ISO/IEC 27001:2005 2013, 27002:2005, 2013, 27799:2008
CFR Part 11
COBIT 4.1
NIST SP 800-53 Revision 4
NIST Cybersecurity Framework (CsF)
DHS Cyber Resilience Review (in CSF v9)

NIST SP 800-66 Revision 1
PCI DSS version 3
FTC Red Flags Rule
FFIEC IT InfoSec Examination (in CSF v9)
201 CMR 17.00 (State of Mass.)
NRS 603A (State of Nev.)

CSA Cloud Controls Matrix version 3.1
CIS CSC version 6 (SANS Top 20)
CMS IS ARS version 2
MARS-E version 2
IRS Pub 1075 v2014
FedRAMP (in CSF v9)

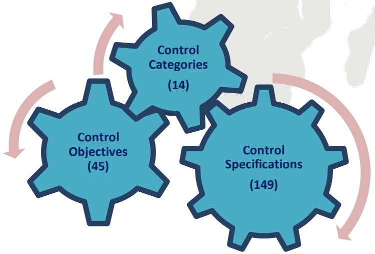
Analyzed, Rationalized & Consolidated

Scoping Factors

Regulatory
- Federal, state and domain specific compliance requirements

Organization
- Geographic factors
- Number of records processed or held

System
- Data stores
- External connections
- Number of users/transactions



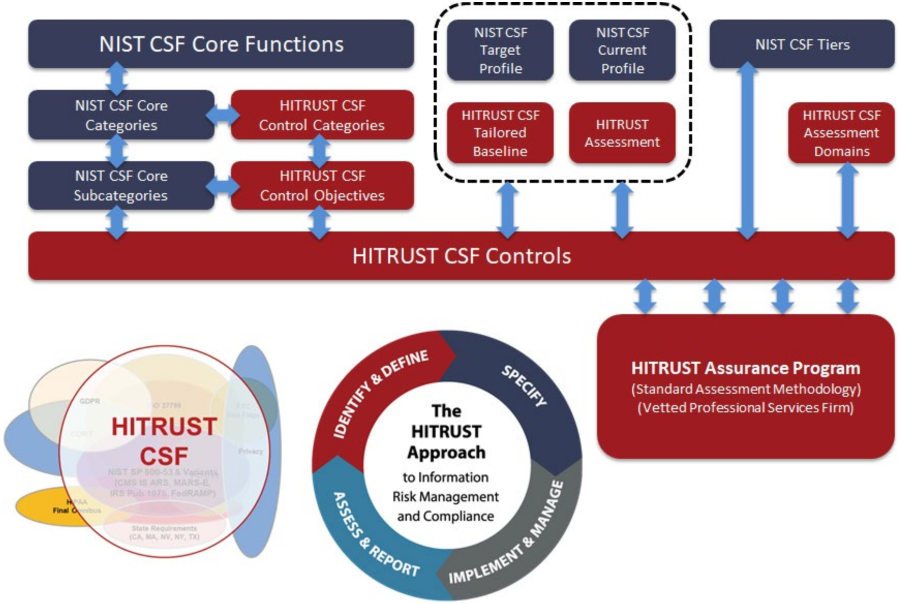
Control Categories

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development & Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

A Model Implementation of the NIST Framework

The HITRUST approach meets or exceeds the NIST requirements, fully addresses non-cyber threats, and incorporates a robust assurance program.

- **Although scalable, the NIST CSF lacks prescription in:**
  - Requirements
  - Assessment methodology
- **… and subsequently lacks:**
  - Accuracy
  - Transparency
  - Consistency
  - Reliability



NIST CSF Core Functions

NIST CSF Core Categories

HITRUST CSF Control Categories

NIST CSF Core Subcategories

HITRUST CSF Control Objectives

NIST CSF Target Profile

NIST CSF Current Profile

HITRUST CSF Tailored Baseline

HITRUST Assessment

NIST CSF Tiers

HITRUST CSF Assessment Domains

HITRUST CSF Controls

HITRUST Assurance Program
(Standard Assessment Methodology)
(Vetted Professional Services Firm)

GDPR
ISO 27799
FTC Red Flags
COBIT
HITRUST CSF
Privacy
NIST SP 800-53 & Variants (CMS IS ARS, MARS-E, IRS Pub 1075, FedRAMP)
HIPAA Final Omnibus
State Requirements (CA, MA, NV, NY, TX)
IDENTIFY & DEFINE
SPECIFY
IMPLEMENT & MANAGE
ASSESS & REPORT
The HITRUST Approach
to Information Risk Management and Compliance

The HITRUST CSF provides the foundation needed to implement the NIST Cybersecurity Framework

4

COMPARING ORGANIZATIONS

Comparing Standards Organizations

Criterion	Response	ANSI	EHNAC	HITRUST	ISACA	ISO	NIST	PCI
Establishes Security Standards	(Y/N)	Y	Y*	Y	Y	Y	Y	Y
Standards Accepted by Industry	(Y/N)	Y	Y	Y^	Y	Y	Y	Y
"Not for Profit" Organization	(Y/N)	Y[1]	Y[2]	Y[2]	Y[2]	Y[3]	Y[4]	Y[1]
Standards are Copyrighted	(Y/N)	Y	Y	Y	Y	Y	N	Y
Standards Free to Implementing Entity	(Y/N)	N	Y	Y#	N	N	Y	Y
Industry Oversight	(Y/N)	Y	Y	Y%	Y	Y	N	Y
Certifiable/Accreditable Standards	(Y/N)	Y	Y	Y	N	Y	Y&	Y

* Adopted the HITRUST CSF® as the security standard for its 18 accreditation programs

^ Most widely used controls framework in healthcare (http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf)

[1] Private, non-profit; special status with U.S. Gov't

[2] Private, non-profit

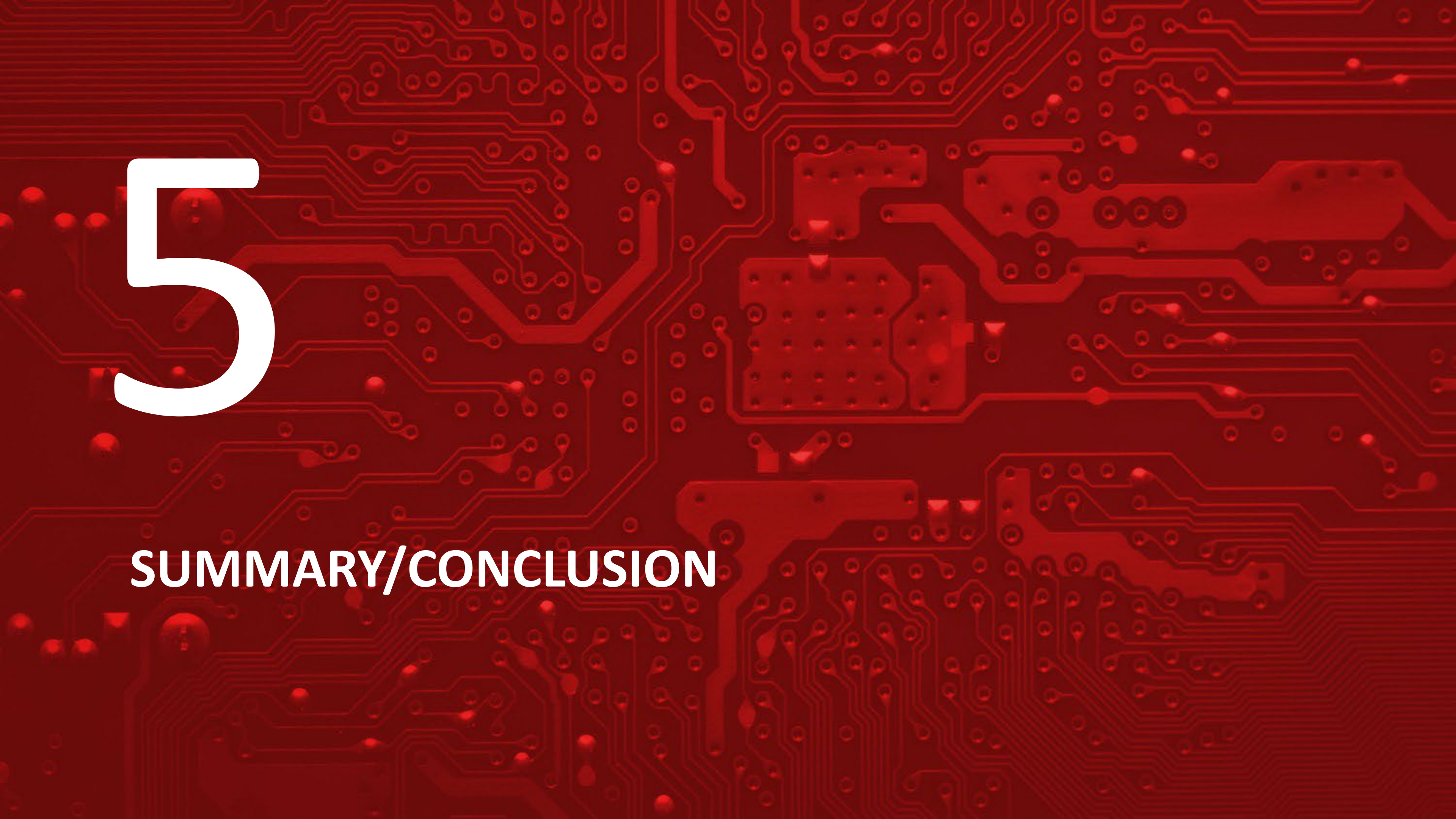
[3] Private, non-profit; special status with U.N.

[4] Government Agency

# Free to qualified entities, which are those organizations that implement the standard as part of their internal information protection program

% Oversight provided by the CSF Advisory Council, which includes such organizations as AHIP, AHA, AMA, AMGA, EHNAC, and TMA

& Government agencies and contractors only



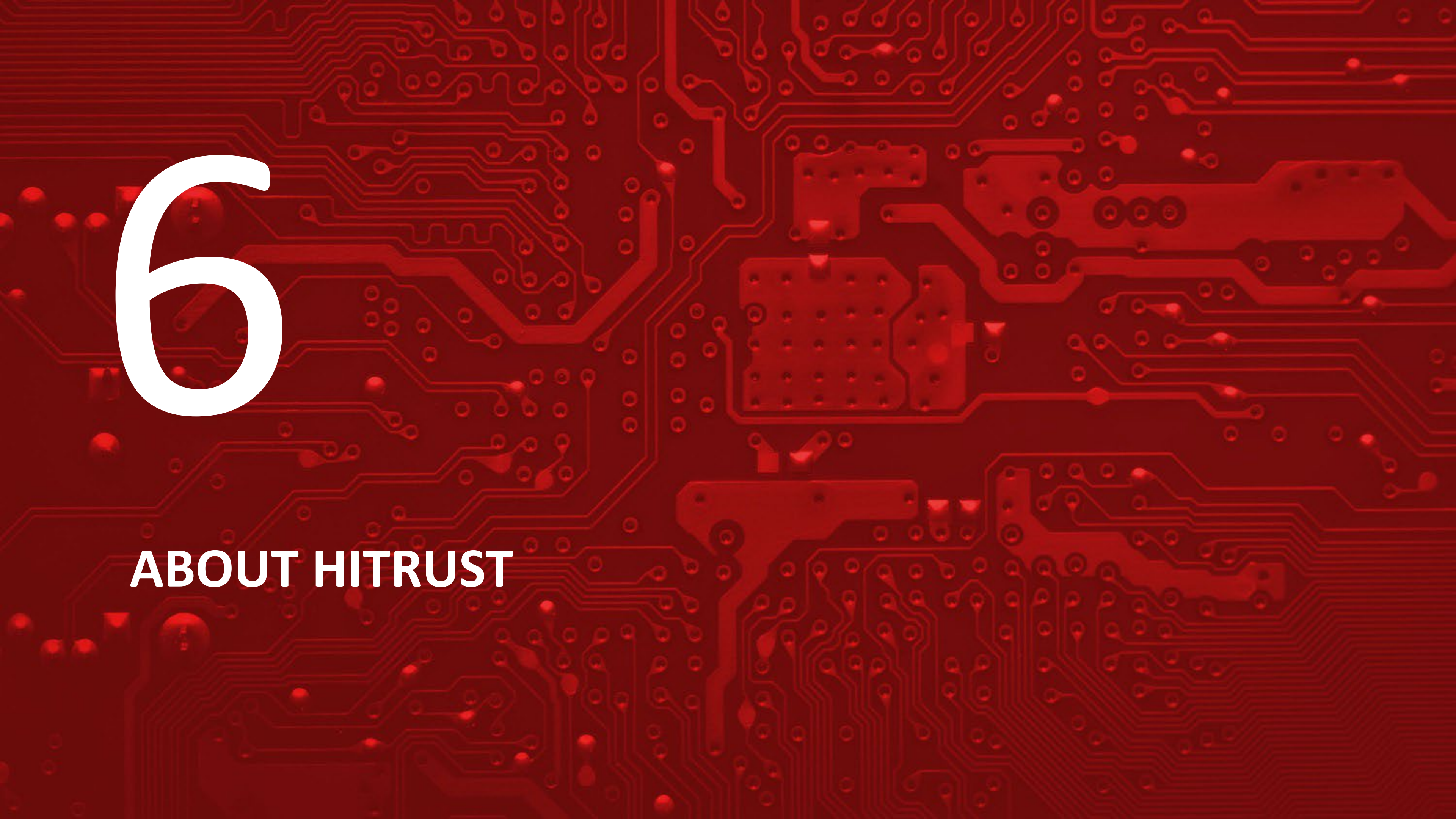
5

SUMMARY/CONCLUSION

Summary/Conclusion

HITRUST is a not-for-profit organization providing information security and privacy requirements/standards that are:

- Widely used within any industry
- Copyrighted consistent with other standards bodies
- Free to obtain/use by implementing organizations, unlike many other standards bodies
- Provided industry oversight consistent with other standards bodies
- Leverages industry working groups/committees consistent with other standards bodies



6

ABOUT HITRUST

BACKGROUND

Since 2007, HITRUST, a leading data protection standards development and certification organization, has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain.

ADOPTION

81%	of US hospitals and health systems utilize the HITRUST CSF
83%	of US health plans utilize the HITRUST CSF
80%	of top cloud service providers use the HITRUST CSF
75%	of Fortune 20 Companies utilize the HITRUST CSF
BEST PRACTICE FOR ASSURANCE	HITRUST Assurance Program is regarded as the best practice for assurance and for assessing third party risk
HUNDREDS OF THOUSANDS	Hundreds of thousands of HITRUST Assessments performed

HITRUST®
SNAPSHOT

BEST KNOWN FOR

The leader in movement towards ***One Framework, One Assessment, Globally***™

Development of a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.

Creating the HITRUST CSF, integrating ~40 authoritative sources and founded on ISO 27001

An assurance program built upon the principles of integrity, transparency, and consistency to ensure that report recipients can understand and rely on the findings

Creating a best in class Software as a Service (SaaS) information risk management platform for assessing and reporting information risk and compliance,

SOLUTIONS

HITRUST CSF®
HITRUST MyCSF®
HITRUST Threat Catalogue®
HITRUST Assessment XChange™
HITRUST Academy®
HITRUST RightStart Program™
HITRUST Third-Party Assurance Program
HITRUST Shared Responsibility Program
HITRUST Assurance Program
HITRUST Venture Program

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Download Center