The Future of HITRUST

Henry Vynalek, Director, HIE & IT Operations and Security Officer

Mike Wells, Director of Security, Director of Engineering

HIMSS CENTRAL & SOUTHERN OHIO Chapter

The Ohio Health Information Partnership (CliniSync)

Henry Vynalek

- Director of HIE & IT Operations
- Security Officer

The Health Collaborative

Mike Wells

- Director of Security
- Director of Engineering

Overview

- Company introductions
- General HITRUST requirements and challenges
- Driving factors for certification
- Company-specific security issues
- Future of HITRUST and added benefits

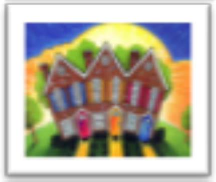
CliniSync At-A-Glance

General

Statistics based on end-of-year 2017

15,000,000 Indexes in the MPI

2,000,000 Clinical Messages per Day



156 hospitals and **500** long term care and post acute care facilities included

7 Payers

***Vendor:** Medicity (Health Catalyst)*

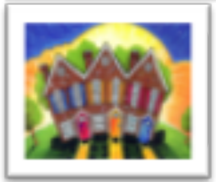
CliniSync At-A-Glance

Services

Statistics based on end-of-year 2017

CHR Community Health Record

Data Mart



Clinical Results Delivery

HIPAA Secure DIRECT Messaging

Public Health Reporting

Medicity and HITRUST

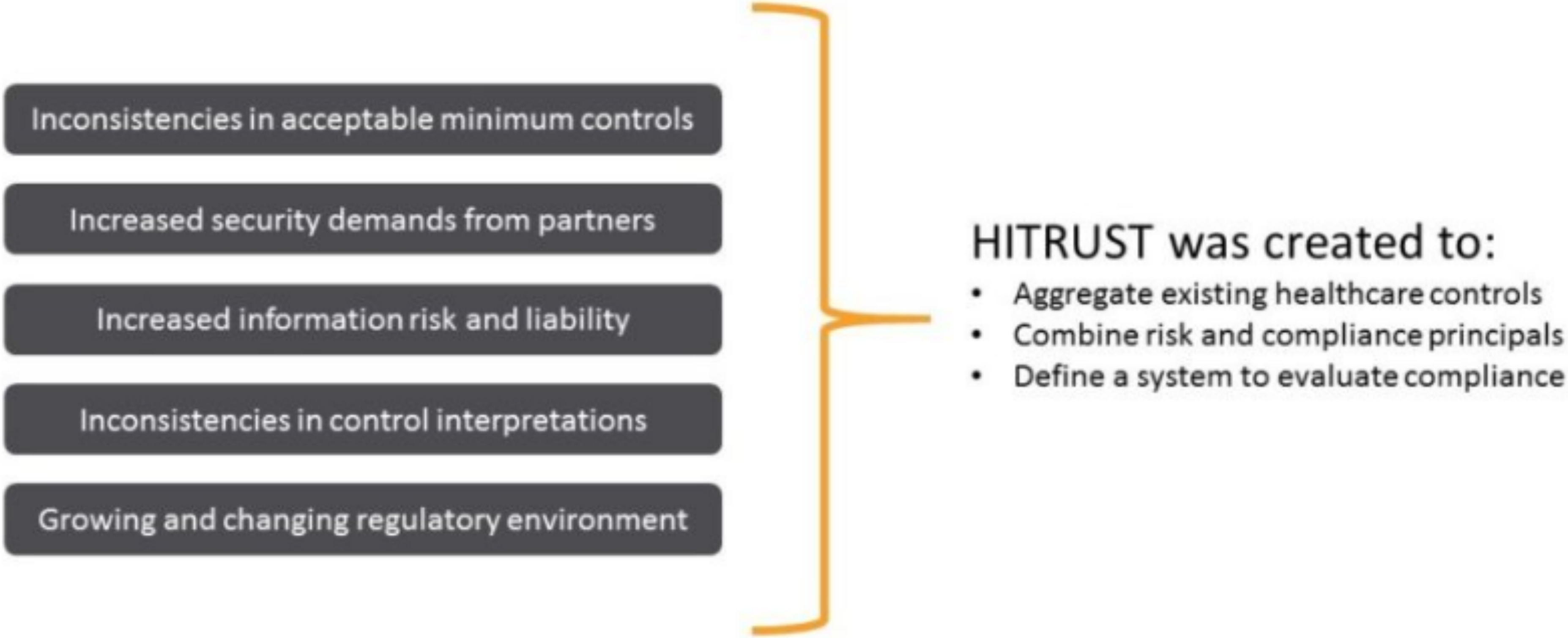
- ➢ HITRUST Certified
- ➢ Contracted Datacenter (ViaWest) also HITRUST Certified

Medicity Data Specs:

- Hyperconverged infrastructure
  - o On-the-fly scalability
- ~2PB combined data
- 100+ VMs
- Using NoSQL to store data
- All CliniSync data resides within Medicity-contracted datacenters

PAYERS

Brief History of HITRUST



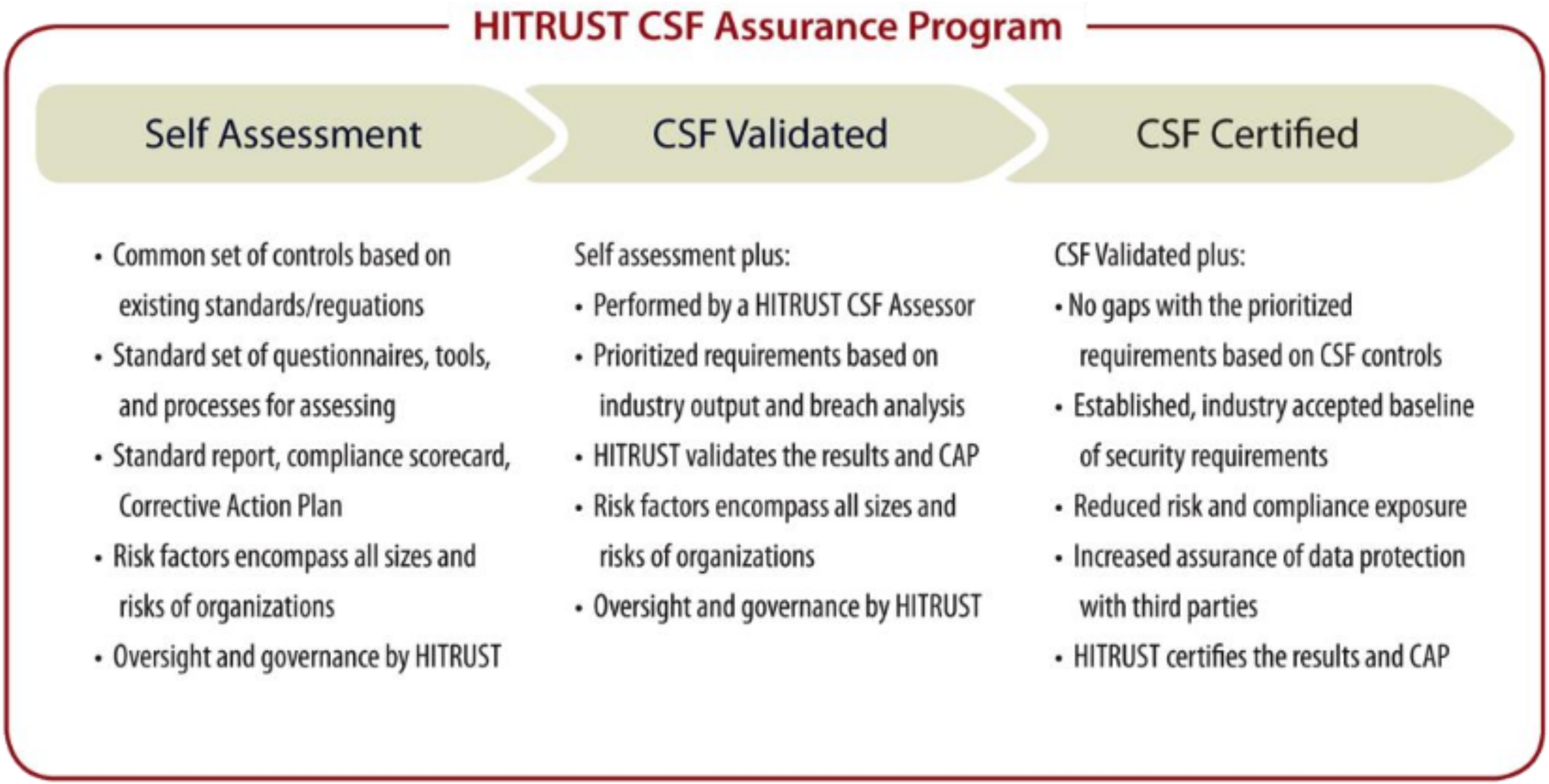
- Inconsistencies in acceptable minimum controls
- Increased security demands from partners
- Increased information risk and liability
- Inconsistencies in control interpretations
- Growing and changing regulatory environment

HITRUST was created to:

- Aggregate existing healthcare controls
- Combine risk and compliance principals
- Define a system to evaluate compliance

Image credit: Brittany Schatz, FRSECURE https://frsecure.com/blog/hitrust-101-hitrust-right-for-you/

Current State of Certification Process



HITRUST CSF Assurance Program

Self Assessment

- Common set of controls based on existing standards/reguations
- Standard set of questionnaires, tools, and processes for assessing
- Standard report, compliance scorecard, Corrective Action Plan
- Risk factors encompass all sizes and risks of organizations
- Oversight and governance by HITRUST

CSF Validated

Self assessment plus:

- Performed by a HITRUST CSF Assessor
- Prioritized requirements based on industry output and breach analysis
- HITRUST validates the results and CAP
- Risk factors encompass all sizes and risks of organizations
- Oversight and governance by HITRUST

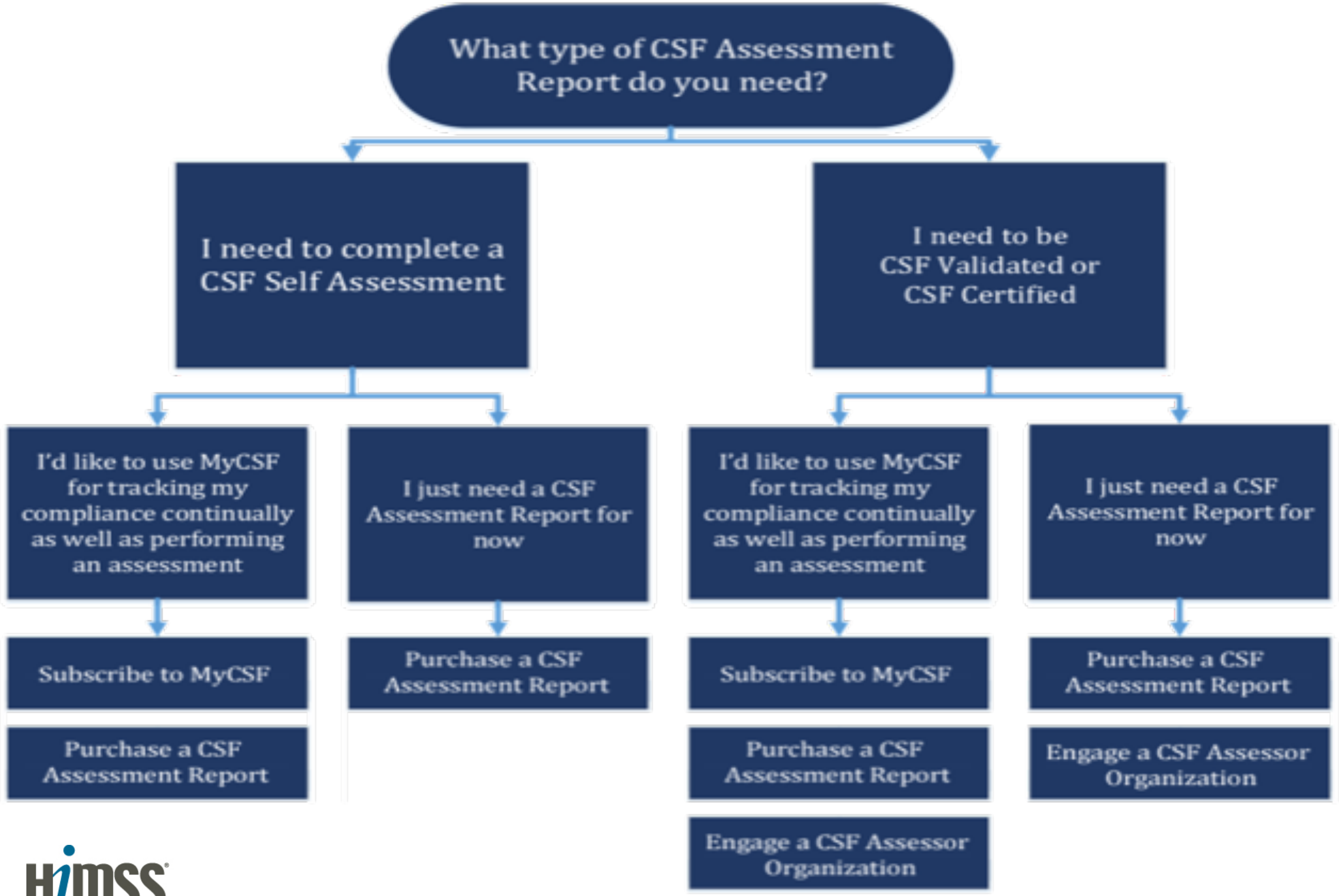
CSF Certified

CSF Validated plus:

- No gaps with the prioritized requirements based on CSF controls
- Established, industry accepted baseline of security requirements
- Reduced risk and compliance exposure
- Increased assurance of data protection with third parties
- HITRUST certifies the results and CAP

Image credit: HITRUST Alliance https://hitrustalliance.net/content/uploads/2014/04/BA-1-Understand-the-CSF-and-CSF-Assurance-Program.pdf

Types of CSF Assessments



What type of CSF Assessment Report do you need?

- I need to complete a CSF Self Assessment
  - I'd like to use MyCSF for tracking my compliance continually as well as performing an assessment
    - Subscribe to MyCSF
    - Purchase a CSF Assessment Report
  - I just need a CSF Assessment Report for now
    - Purchase a CSF Assessment Report
- I need to be CSF Validated or CSF Certified
  - I'd like to use MyCSF for tracking my compliance continually as well as performing an assessment
    - Subscribe to MyCSF
    - Purchase a CSF Assessment Report
    - Engage a CSF Assessor Organization
  - I just need a CSF Assessment Report for now
    - Purchase a CSF Assessment Report
    - Engage a CSF Assessor Organization

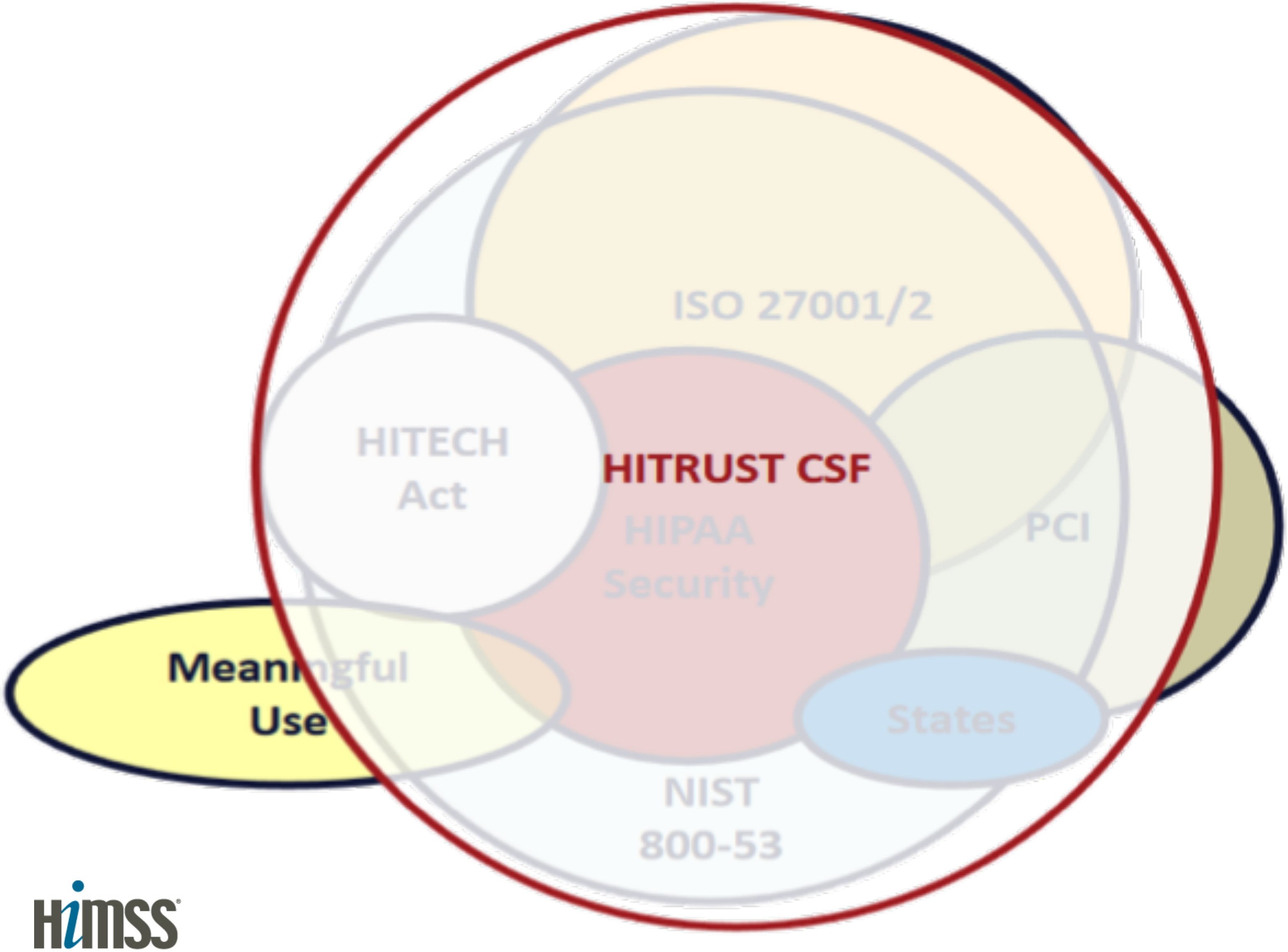
Image Credit: HITRUST, https://hitrustalliance.net/assessment-right/

HITRUST Areas Evaluated

- Information Protection Program
- Endpoint Protection
- Portable Media Security
- Mobile Device Security
- Wireless Protection
- Configuration Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Password Management

- Access Control
- Audit Logging & Monitoring
- Education, Training & Awareness
- Third Party Security
- Incident Management
- Business Continuity & Disaster Recovery
- Risk Management
- Physical & Environmental Security
- Data Protection & Privacy

Bridging the CSF Gap



HIMSS CENTRAL & SOUTHERN OHIO *Chapter*

Image credit: HITRUST, https://hitrustalliance.net/content/uploads/2014/04/BA-1-Understand-the-CSF-and-CSF-Assurance-Program.pdf

Benefits of Adopting HITRUST CSF

- Reduced costs and complexity
  - Implementing one CSF vs individual requests
  - Less hours worked on responding to security requests
- Managed risk
  - Increased insight and knowing exactly what each control entails
- Simplified compliance
  - Knowing controls that fit your security requirements

Common Questions and Current State

- **Questions:**
  - Data Loss Prevention (DLP)?
  - Removable Media?
  - Credential management?
  - Internal processes?

- **Current State:**
  - In the self-assessment phase of HITRUST
  - Have chosen an assessor

The Health Collaborative – Who We Are

Began in 1997

~55 Employees

~100 servers (Windows & Linux)

~50 TB SAN

Data:

- 58 hospitals
- 12 payers
- 8900 healthcare providers
- 5 million lives in MPI
- 15 million clinical messages per month

Services:

- Clinical results delivery
- Encounter notification
- Secure direct messaging
- Patient Centered Data Home (PCDH)
- Comprehensive Primary Care (CPC)

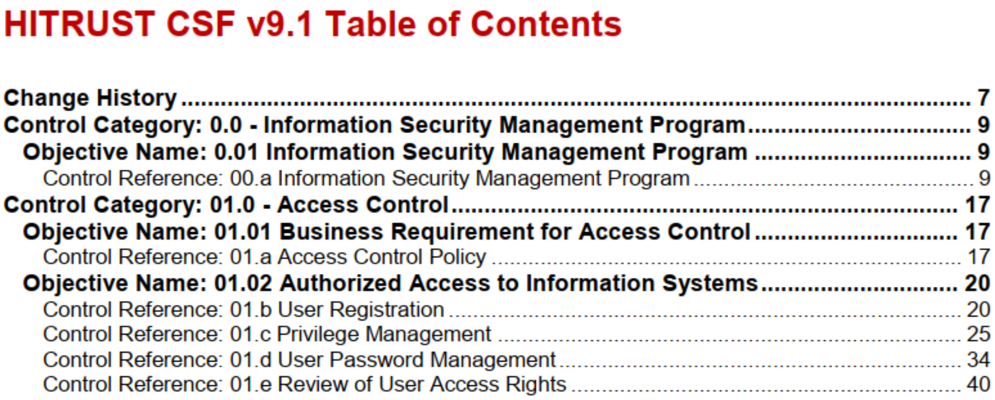
The Health Collaborative – The Journey

- 2012 – information security program begins to be formalized and information security officer position is created.
- NIST 800-53 chosen as security framework
- 2014 - CMS Qualified Entity status obtained
- 2015 - EHNAC certification for DirectTrust participation
- 2017 - HITRUST certification

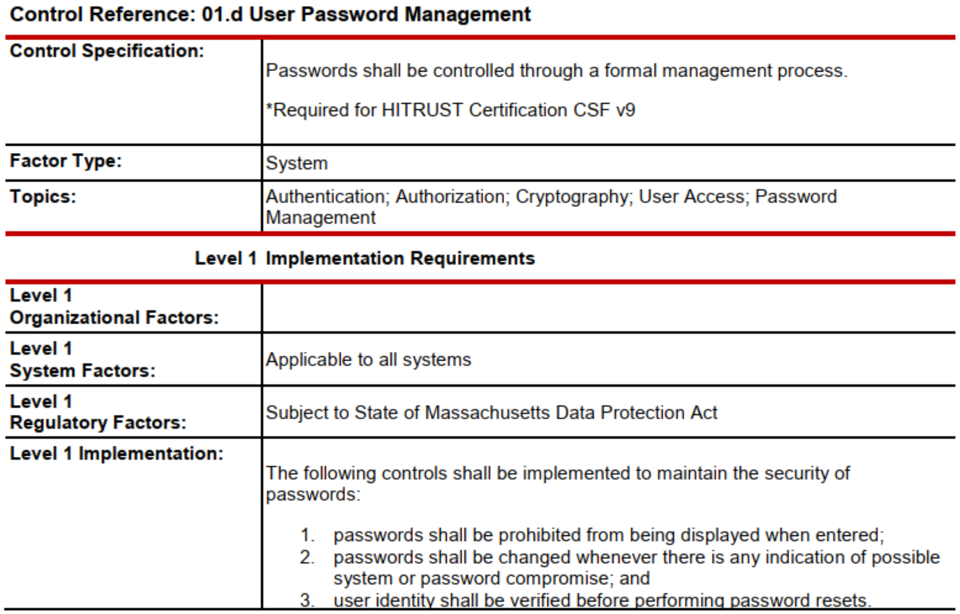
General HITRUST Requirements and Challenges

- Subscribe to MyCSF from HITRUST
- Self assess first?
- What systems are in scope?
- Amount, type of data, system complexity & regulatory requirements
  = risk = depth of assessment
  - Called control factors within MyCSF
  - Includes additional frameworks such as PCI and GDPR
- Select a certified assessor
  - Do you need additional certifications?
- Full assessment every other year with interim (partial) assessment opposite years.

Map policies, procedures and evidence to each control statement



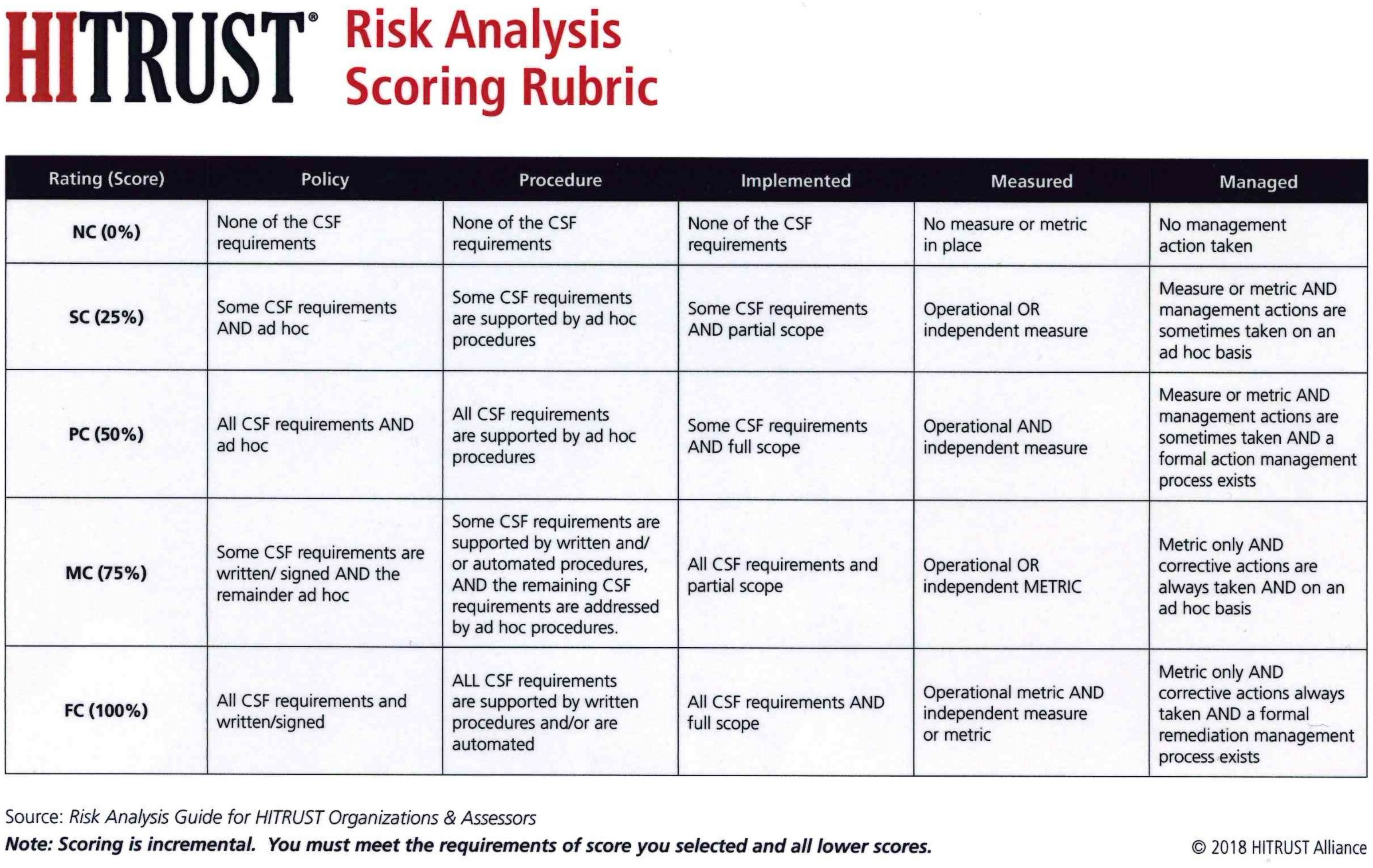
HITRUST CSF v9.1 Table of Contents



Control Reference: 01.d User Password Management

Control Specification:	Passwords shall be controlled through a formal management process. *Required for HITRUST Certification CSF v9
Factor Type:	System
Topics:	Authentication; Authorization; Cryptography; User Access; Password Management
Level 1	**Implementation Requirements**
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	The following controls shall be implemented to maintain the security of passwords: 1. passwords shall be prohibited from being displayed when entered; 2. passwords shall be changed whenever there is any indication of possible system or password compromise; and 3. user identity shall be verified before performing password resets.

Scoring is highly objective



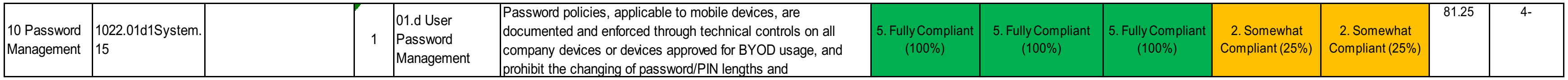
HITRUST® Risk Analysis Scoring Rubric

Rating (Score)	Policy	Procedure	Implemented	Measured	Managed
NC (0%)	None of the CSF requirements	None of the CSF requirements	None of the CSF requirements	No measure or metric in place	No management action taken
SC (25%)	Some CSF requirements AND ad hoc	Some CSF requirements are supported by ad hoc procedures	Some CSF requirements AND partial scope	Operational OR independent measure	Measure or metric AND management actions are sometimes taken on an ad hoc basis
PC (50%)	All CSF requirements AND ad hoc	All CSF requirements are supported by ad hoc procedures	Some CSF requirements AND full scope	Operational AND independent measure	Measure or metric AND management actions are sometimes taken AND a formal action management process exists
MC (75%)	Some CSF requirements are written/ signed AND the remainder ad hoc	Some CSF requirements are supported by written and/ or automated procedures, AND the remaining CSF requirements are addressed by ad hoc procedures.	All CSF requirements and partial scope	Operational OR independent METRIC	Metric only AND corrective actions are always taken AND on an ad hoc basis
FC (100%)	All CSF requirements and written/signed	ALL CSF requirements are supported by written procedures and/or are automated	All CSF requirements AND full scope	Operational metric AND independent measure or metric	Metric only AND corrective actions always taken AND a formal remediation management process exists

Source: *Risk Analysis Guide for HITRUST Organizations & Assessors*

Note: Scoring is incremental. You must meet the requirements of score you selected and all lower scores.

Scoring is highly objective



10 Password Management	1022.01d1System.15		1	01.d User Password Management	Password policies, applicable to mobile devices, are documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and prohibit the changing of password/PIN lengths and	5. Fully Compliant (100%)	5. Fully Compliant (100%)	5. Fully Compliant (100%)	2. Somewhat Compliant (25%)	2. Somewhat Compliant (25%)	81.25	4-

Domain	Total Score	Controls	Average	PRISMA
01 Information Protection Program	2600	32	81.25	4-
02 Endpoint Protection	700	8	87.50	4+
03 Portable Media Security	700	8	87.50	4+
04 Mobile Device Security	900	11	81.82	4-
05 Wireless Security	400	5	80.00	4-
06 Configuration Management	800	10	80.00	4-
07 Vulnerability Management	1600	19	84.21	4
08 Network Protection	3000	32	93.75	5-
09 Transmission Protection	725	9	80.56	4-
10 Password Management	850	13	65.38	3
11 Access Control	1500	37	40.54	2
12 Audit Logging & Monitoring	2700	31	87.10	4+
13 Education, Training and Awareness	1000	14	71.43	3+
14 Third Party Assurance	1500	18	83.33	4
15 Incident Management	2000	25	80.00	4-
16 Business Continuity & Disaster Recovery	400	8	50.00	2+
17 Risk Management	900	11	81.82	4-
18 Physical & Environmental Security	2500	29	86.21	4
19 Data Protection & Privacy	600	7	85.71	4
Totals	**25375**	**327**	**78.32**	

Score	PRISMA
10	1-
19	1
27	1+
36	2-
45	2
53	2+
62	3-
71	3
79	3+
83	4-
87	4
90	4+
94	5-
98	5
100	5+

Driving Factors for Certification

- Required by one of your data providers
- Business driver / marketing
- Reduce or simplify 3rd party risk assessments
- Strengthen your info sec program
- Demonstrate due diligence should something bad happen
- Badge of honor

Future of HITRUST and Added Benefits

- CSF v10 due out in the first half of 2019
- MyCSF 2.0 rolling out any day now
- More granular assessment/certification options based on risk factors and regulatory requirements
- Provider 3rd party risk management program
- Higher industry acceptance.

Am I more secure?

Sure

- Procedures are more rigorously followed and completion is audited
- Corporate security awareness elevated through additional messaging
- Very clear documentation of maturity of each control and control domain.
- Funding for some automation
- Funding for SIEM and DR

Questions??

- **Henry Vynalek**

hvynalek@ohiponline.org

- **Mike Wells**

mwells@healthcollab.org

HIMSS CENTRAL & SOUTHERN OHIO *Chapter*