Crowe

Smart decisions. Lasting value.™

Double the value: SOC 2+ reporting

April 13, 2021

Presented by:
Arshad Ahmed
Jaclyn Dettloff
Vikas Sharma

Your Presenters

Arshad Ahmed
Partner, IT Assurance Services
Partner-in-Charge, SOC Solutions
arshad.ahmed@crowe.com

Jaclyn Dettloff
Senior Manager, IT Assurance Services
jaclyn.dettloff@crowe.com

Vikas Sharma
Senior Manager, IT Assurance Services
vikas.sharma@crowe.com

Agenda

01 Third-party assurance landscape

02 Overview of SOC 2+ reporting option

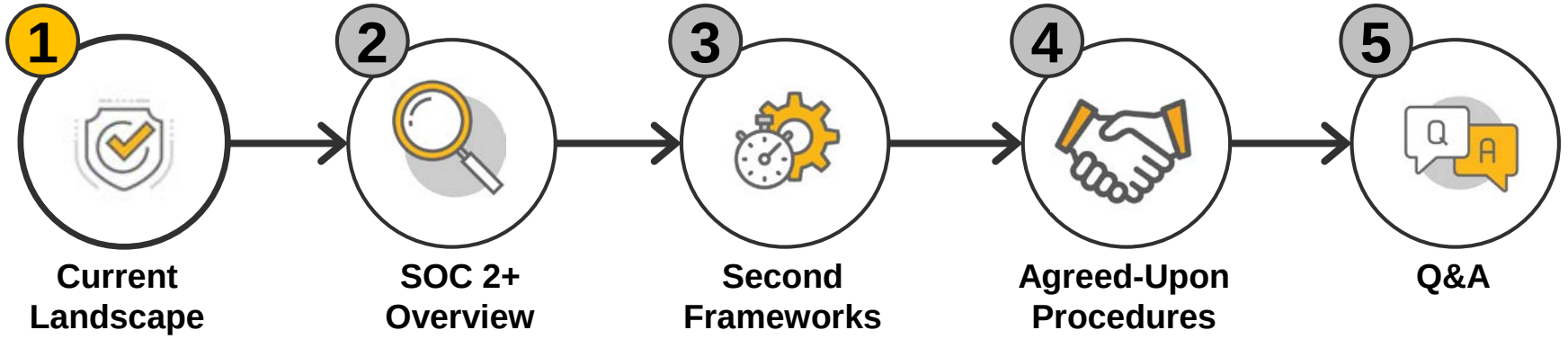
03 Choosing a second framework

04 Agreed-upon procedures option

05 Questions and Closing

Third-party assurance

Current landscape



Building trust through assurance

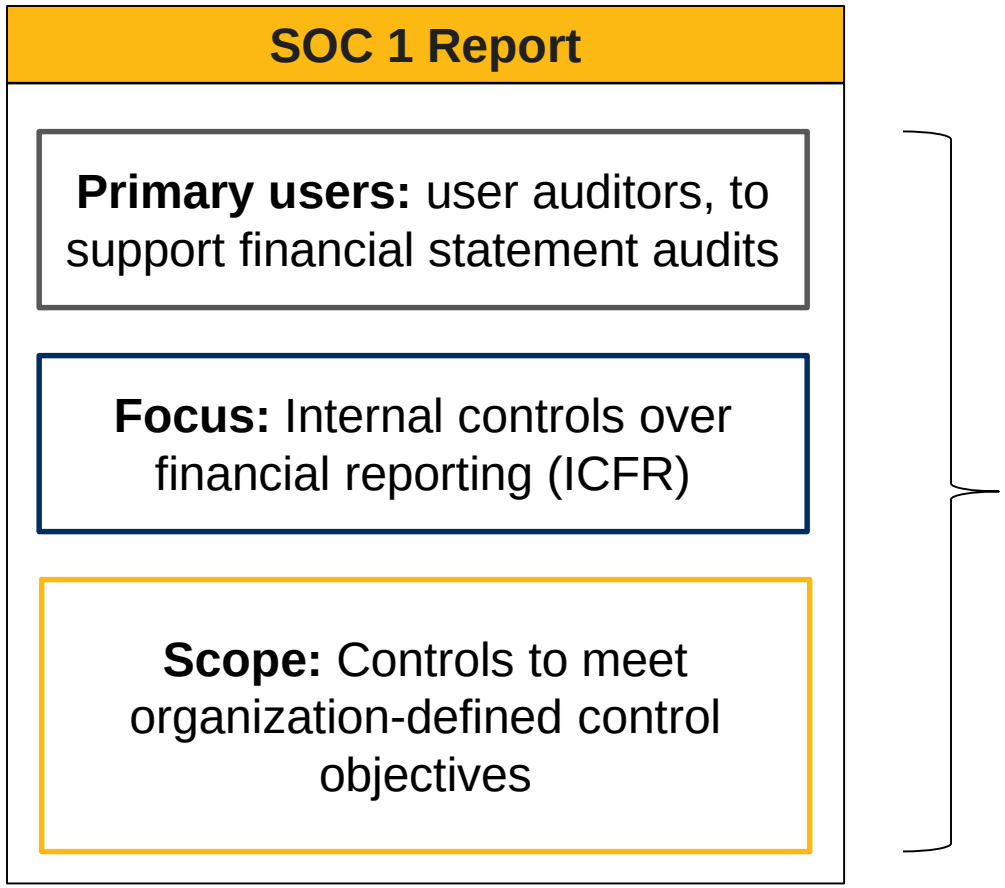
Drivers for third-party assurance reporting

Differentiate from their peers and expand market reach

Meet due diligence and contractual requirements

Demonstrate the maturity of information security program and technology practices

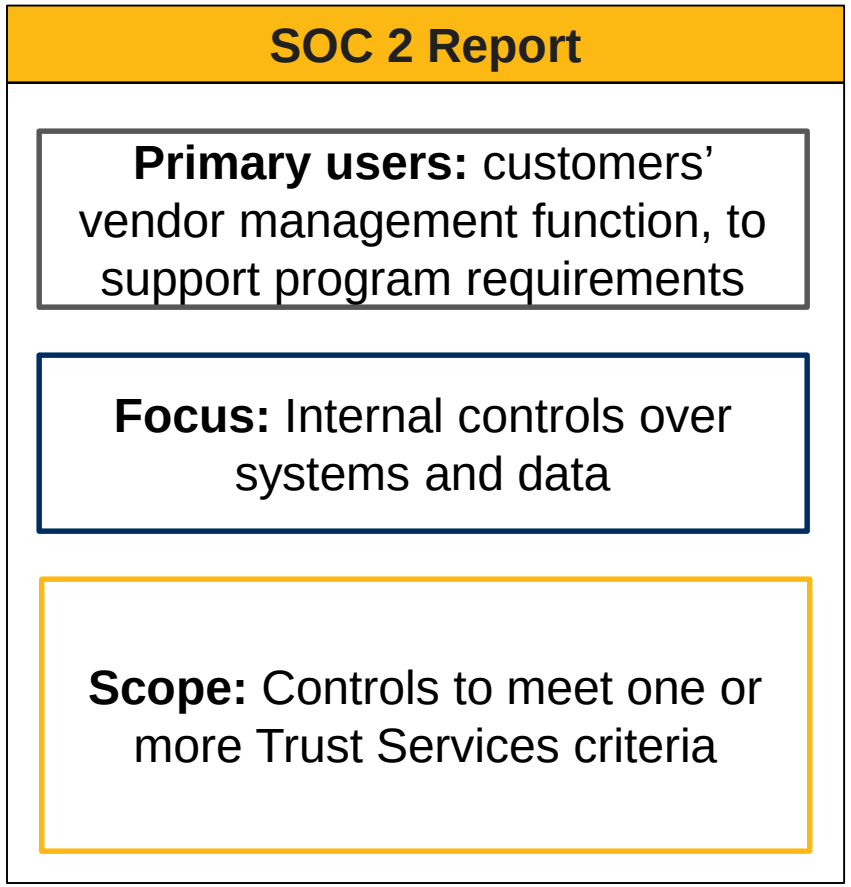
SOC reporting



Objective is to address customers' risks related to ICFR – typical coverage areas:

- ✓ Account setup and maintenance
- ✓ Transaction processing
- ✓ System and data integrity (ITGCs)
- ✓ Report outputs

SOC reporting



Can address wider IT-related concerns, including:

- ✓ Security of systems and data
- ✓ System availability and data recoverability
- ✓ Processing integrity and accuracy (includes non-financial data)
- ✓ Safeguards to protect sensitive data
- ✓ Data privacy: collection, use and disclosure of PII

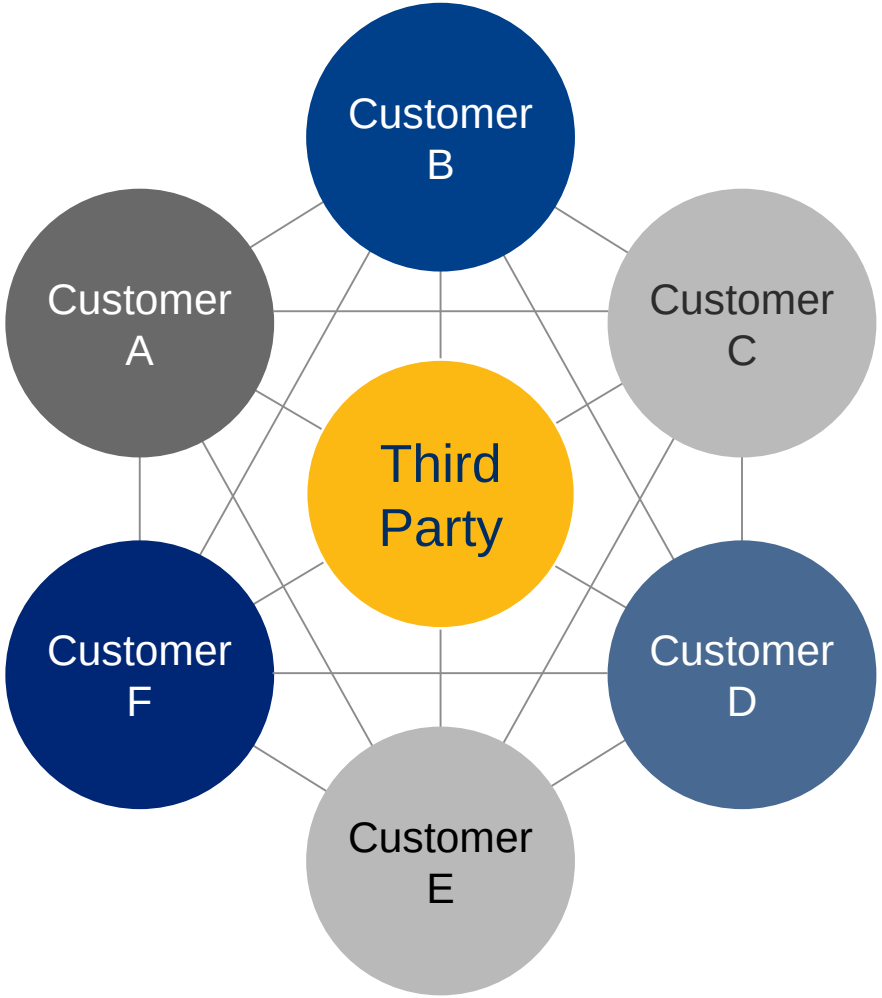
Current landscape

Challenges faced by **third parties**:

- Unique security requirements
- Inability to leverage questionnaire responses across customers
- Time-intensive customer audits

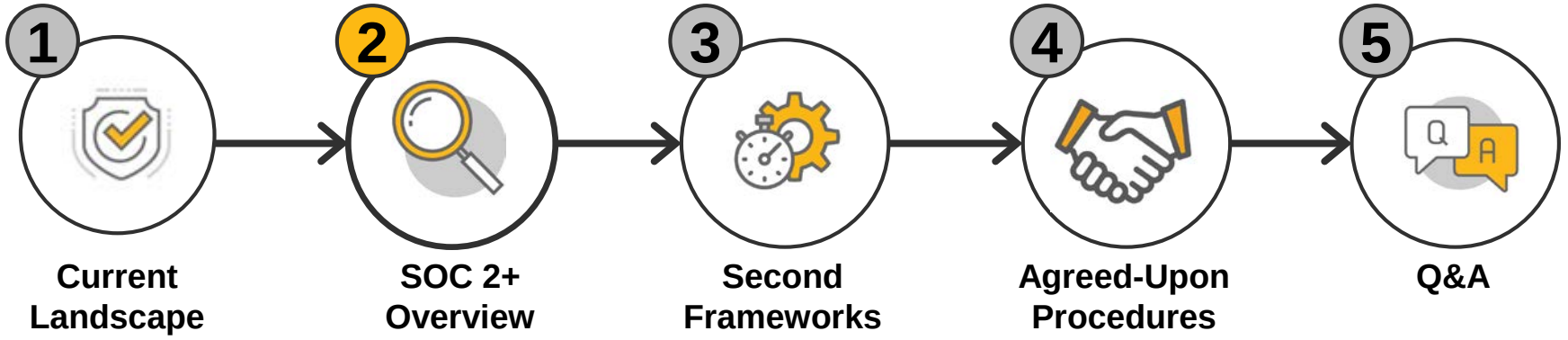
Challenges faced by **customers**:

- Effort to chase down questionnaire responses
- Complexity to evaluate responses
- Lower assurance (responses not validated)



SOC 2+ reporting

Overview and key differences



SOC 2+ overview

SOC 2+ at a Glance…

Scope and Effort

SOC 2 Trust Services Criteria and second industry framework

Key Features

- ✓ Leverages recognition of SOC 2
- ✓ Conducted according to AICPA SOC 2 examination procedures
- ✓ Provides more comprehensive view of internal controls

Deliverable

SOC 2 report, covering both frameworks, that includes:

- Opinion on control design and effectiveness over a period
- Description of controls
- Control test procedures and results

SOC 2+ report deliverable

Illustrative SOC 2 Opinion

To **Company ABC**

Scope

We have examined **Company ABC's** accompanying description of its **XYZ Solutions** system… throughout the period **January 1, 2021 to September 30, 2021**… and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that **Company ABC's** service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria).

Opinion

In our opinion, in all material respects:

a. the description presents **Company ABC's XYZ Solutions** system that was designed and implemented throughout the period **January 1, 2021 to September 30, 2021**, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period **January 1, 2021 to September 30, 2021**, to provide reasonable assurance that **Company ABC's** service commitments and system requirements would be achieved based on the applicable trust services criteria...

c. the controls stated in the description operated effectively throughout the period **January 1, 2021 to September 30, 2021,** to provide reasonable assurance that **Company ABC's** service commitments and system requirements were achieved based on the applicable trust services criteria...

Illustrative SOC 2+ Opinion

To **Company ABC**

Scope

We have examined **Company ABC's** accompanying description of its **XYZ Solutions** system… throughout the period **January 1, 2021 to September 30, 2021**… and the suitability of the design and operating effectiveness of controls stated in the description throughout the period **January 1, 2021 to September 30, 2021**, to provide reasonable assurance that **Company ABC's** service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria), and the requirements set forth in the HIPAA Security Rule (HIPAA criteria).

Opinion

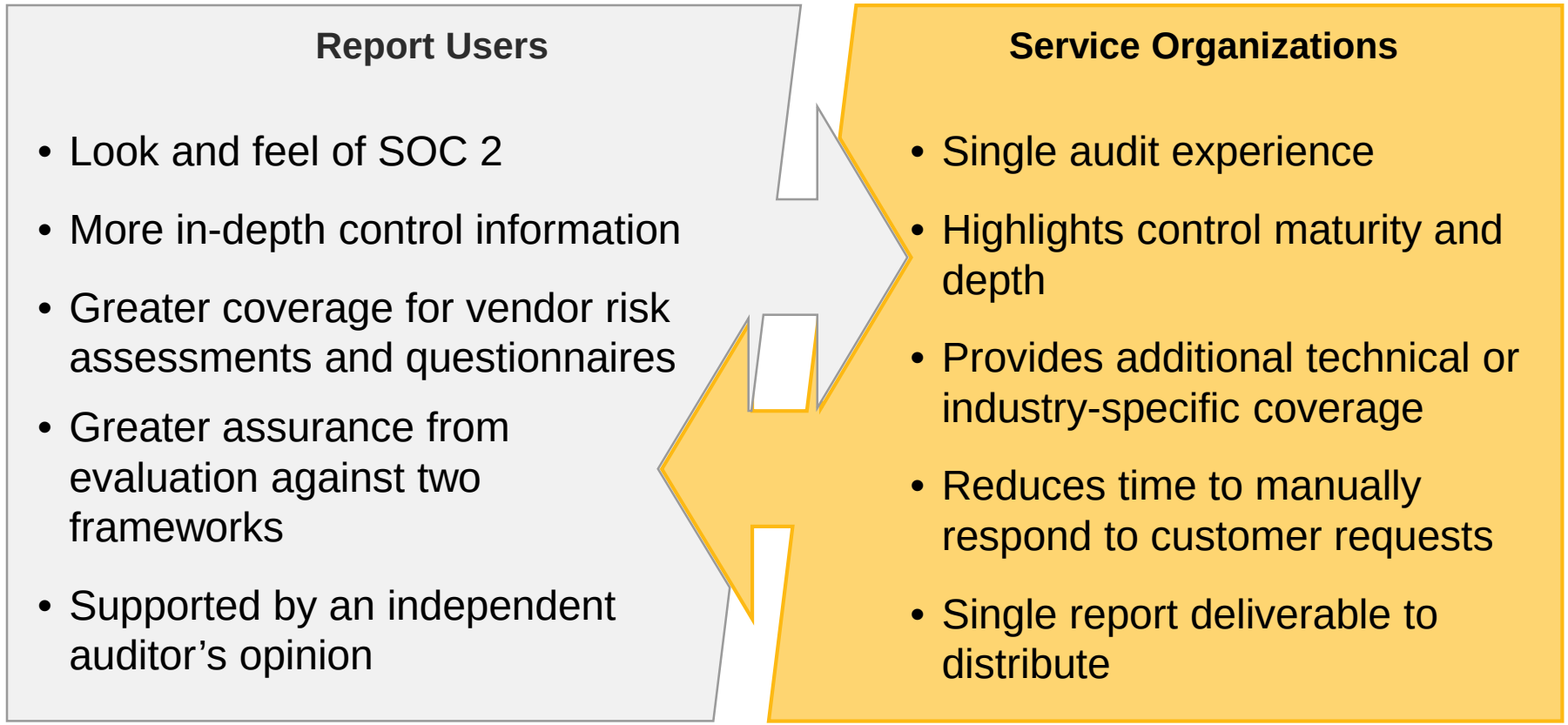
In our opinion, in all material respects:

a. the description presents **Company ABC's XYZ Solutions** system that was designed and implemented throughout the period **January 1, 2021 to September 30, 2021**, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period **January 1, 2021 to September 30, 2021**, to provide reasonable assurance that **Company ABC's** service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA Security Rule criteria...

c. the controls stated in the description operated effectively throughout the period **January 1, 2021 to September 30, 2021,** to provide reasonable assurance that **Company ABC's** service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA Security Rule criteria...

Benefits of SOC 2+



Incremental effort

Common Criteria		
Information Security Program	Legal and Compliance	Network Security
IT Risk Management	Logical Security	Data Center Operations
Human Resources	Data Protection	Change Management

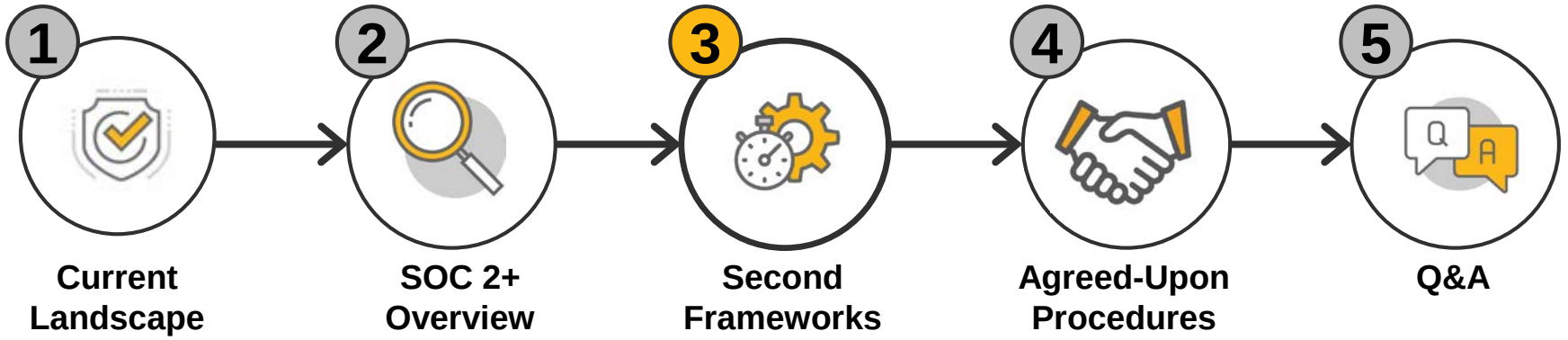
Confidentiality	Privacy	Processing Integrity
Data Retention and Deletion	Privacy Notice and Consent	Input Validation
Data Backups and Replication	PII Collection, Use and Disclosure	Data Processing
Continuity and Disaster Recovery	Handling Data Subject Inquiries	Output Controls

Availability

Typically, **20-50%** additional controls needed to address second framework

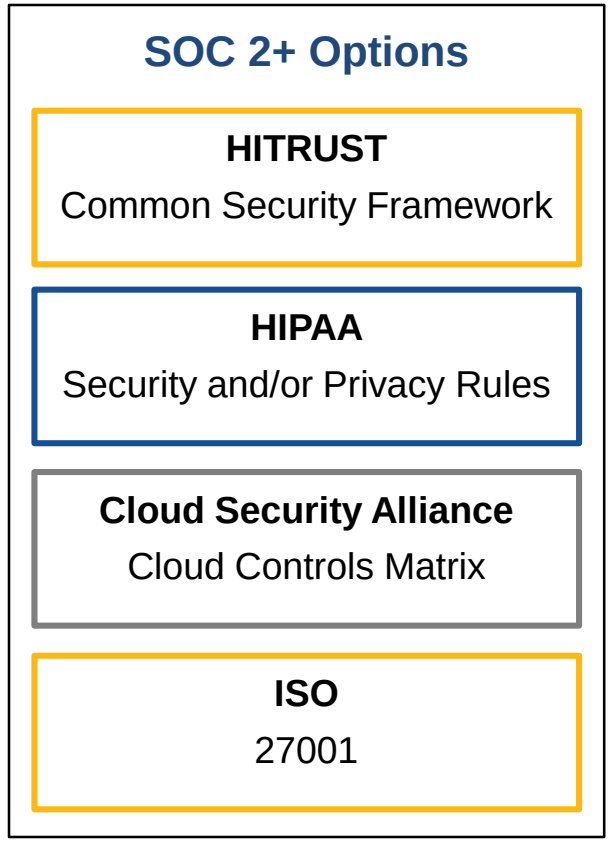
Choosing your ‘+’

Second framework options

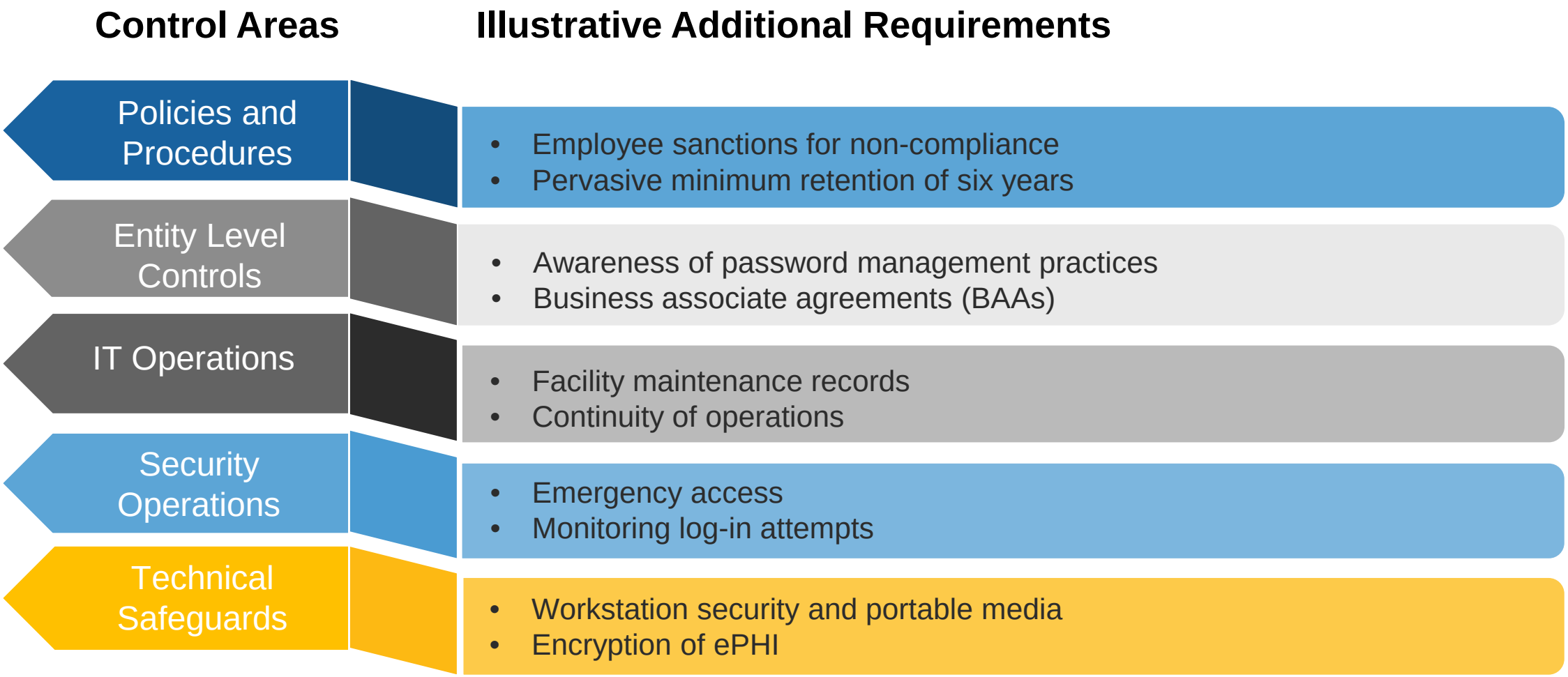


Commonly used frameworks

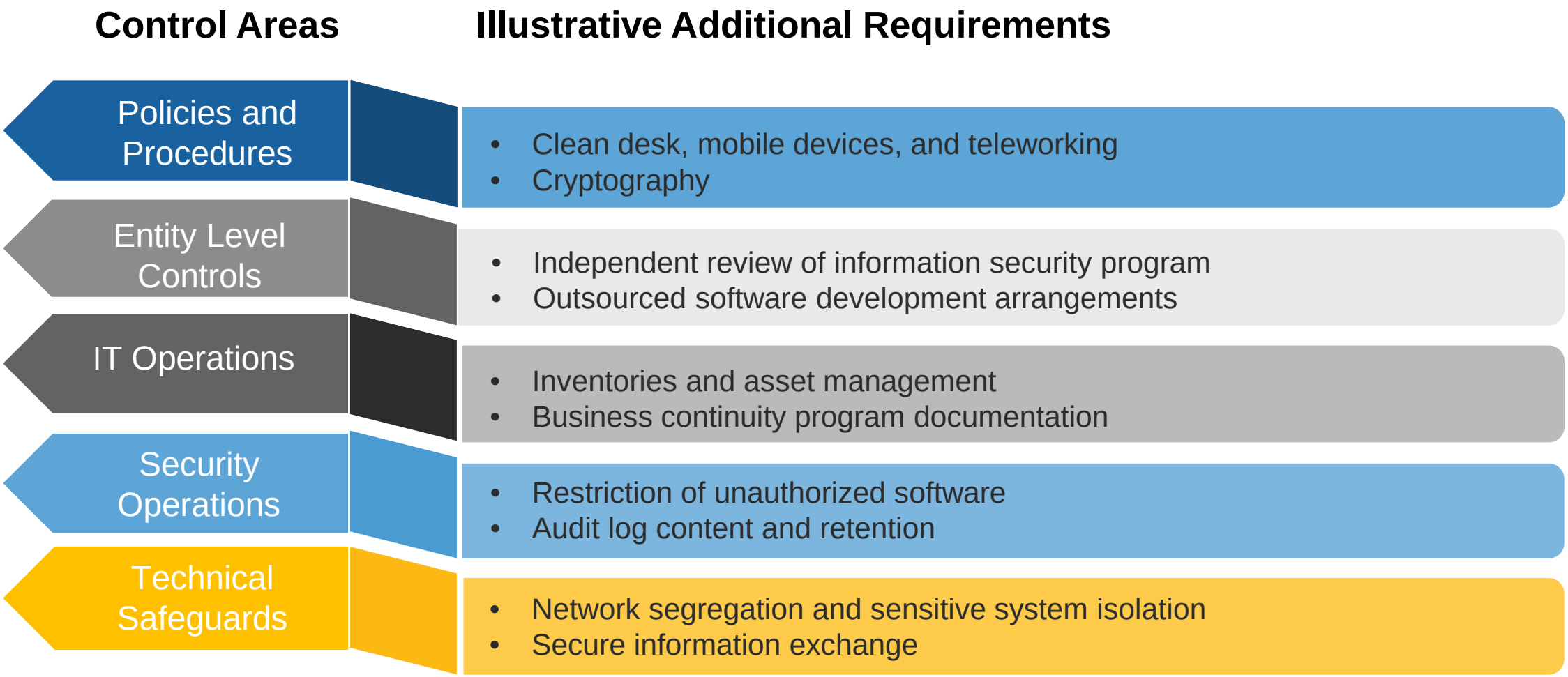
- Any existing control framework can be used
  - ✓ Part of SOC 2 report: opinion on control design and operating effectiveness
  - ✓ Most common SOC 2+ options noted at right
- Framework with IT / security focus recommended
  - ✓ Related subject matter: common relevance, common report users
  - ✓ Common areas of coverage between two frameworks



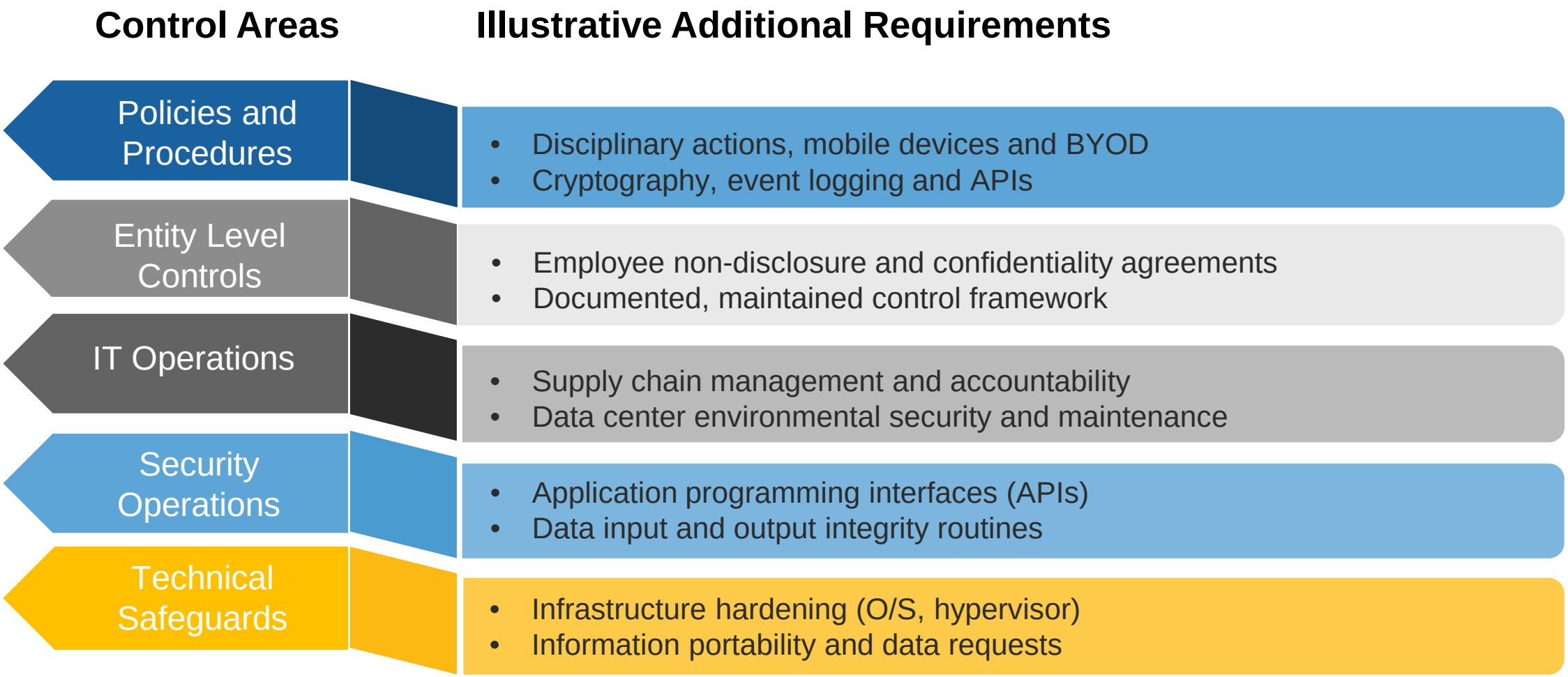
SOC 2 + | HIPAA Security Rule



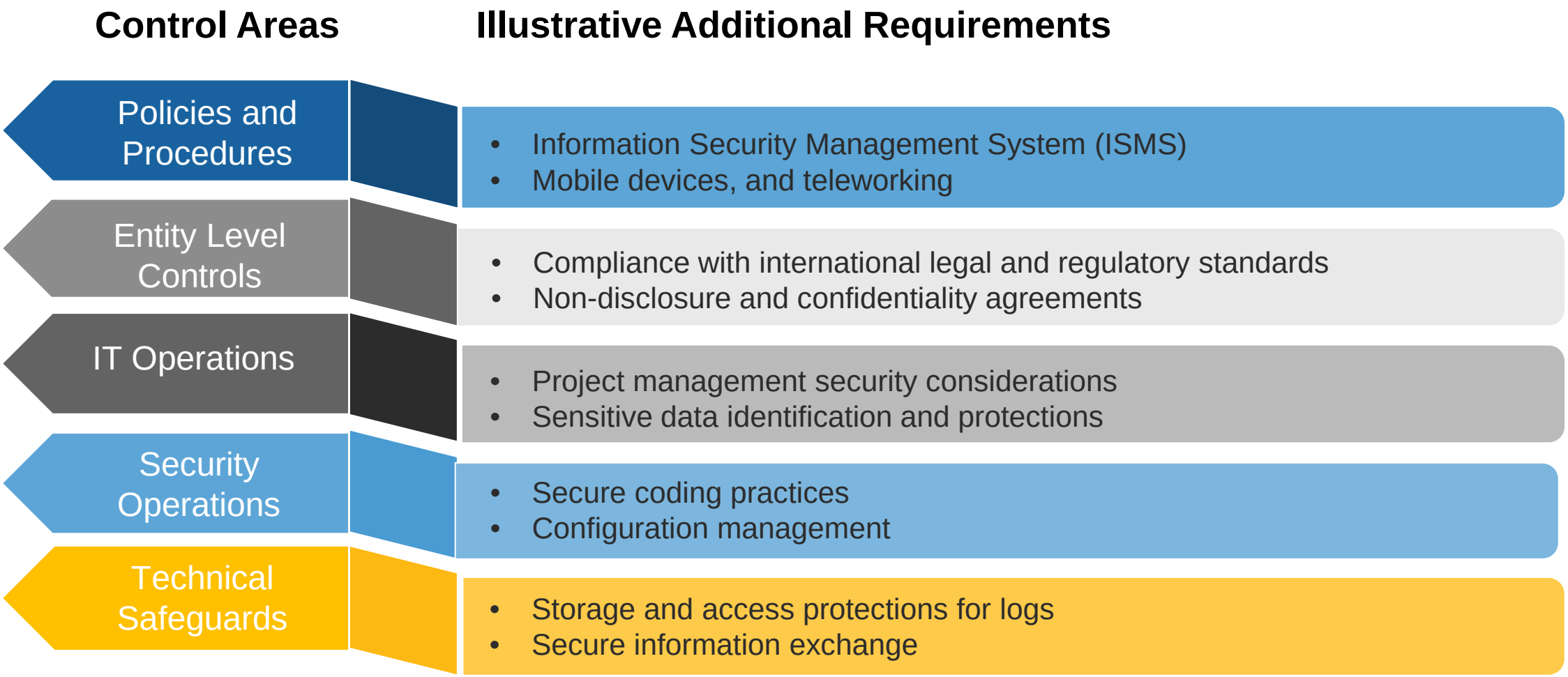
SOC 2 + | HITRUST CSF



SOC 2 + | Cloud Security Alliance CCM



SOC 2 + | ISO 27001



Framework Summary

HIPAA Security Rule

- Security standards to protect PHI
- Demonstrates HIPAA compliance – management, customers and regulators

Typically, **10-15%** additional controls

HITRUST CSF**

- Comprehensive information protection framework
- Highlights more in-depth technical safeguards
- Resonates with healthcare customers

Typically, **25-35%** additional controls

**Does not provide certification

ISO 27001**

- Global information security standard
- Demonstrates ongoing management and improvement of information security program
- Resonates with international customers and within technology industry

Typically, **20-25%** additional controls

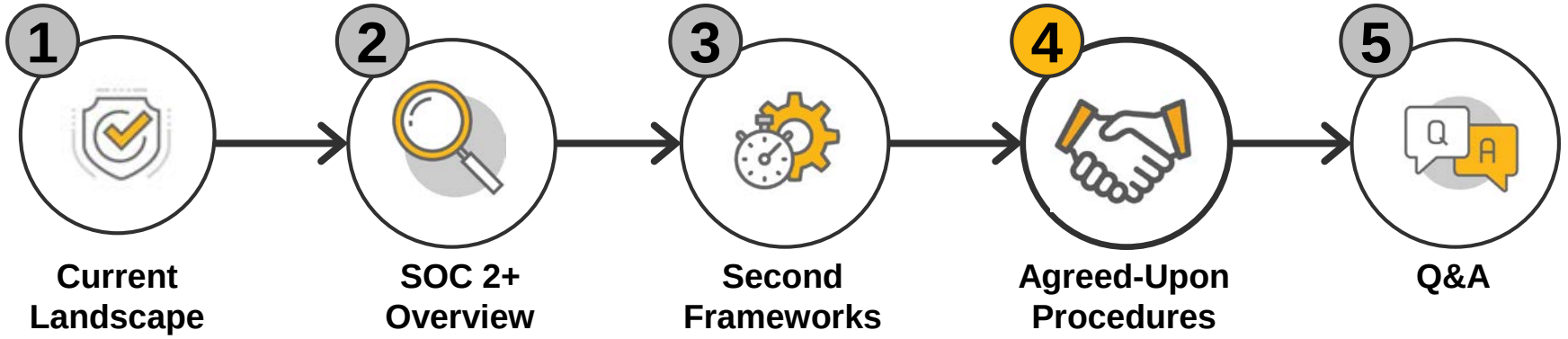
CSA Cloud Controls Matrix**

- Security standards for cloud providers
- Tailored to cloud computing risks and practices
- Acknowledges and addresses specific security risks for cloud providers

Typically, **30-50%** additional controls

Agreed-upon procedures

A closer look



Agreed-Upon Procedures

AUPs at a Glance…

Scope and Effort

Custom scope of procedures, can be determined by organization and/or CPA firm

Deliverable

Attestation report that includes:

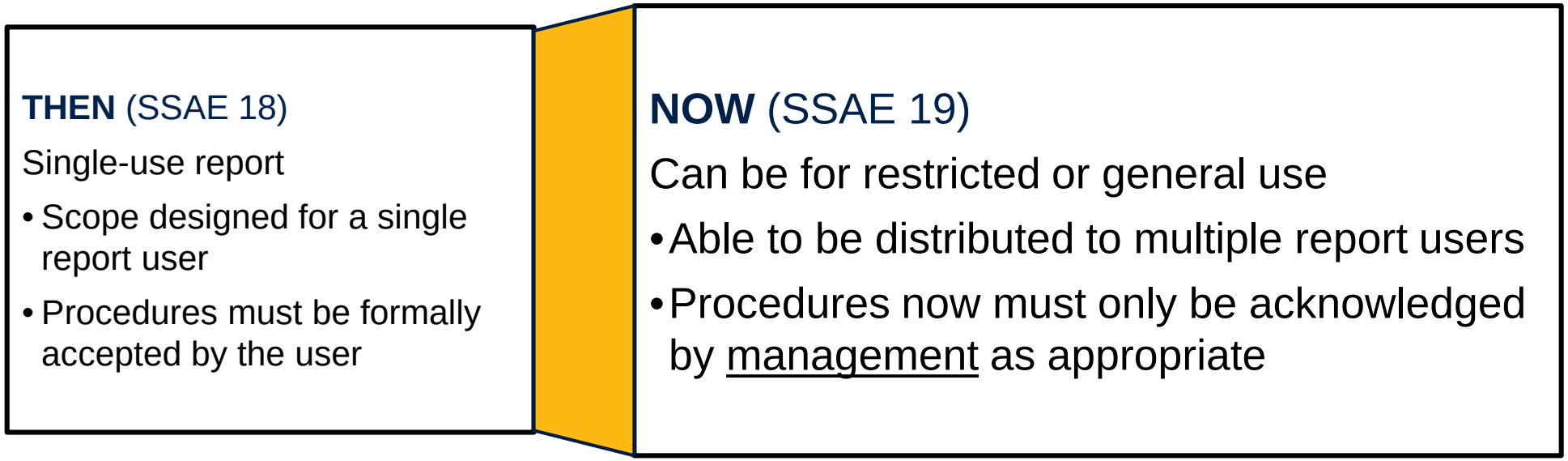
- Independent practitioner's report
- Detailed procedures and results

Key Considerations

- ✓ Fully custom scope (no framework as basis)
- ✓ Very detailed procedures – best positioned to meet customer needs
- ✓ Market awareness: customer education may be needed
- ✓ Does not provide an opinion; only factually reports results of procedures

Agreed-Upon Procedures

- Existing type of AICPA attestation engagement
- Report deliverable includes:
  - ✓ Independent practitioner's report
  - ✓ Detailed procedures and results



Q&A: Open Discussion

Thank You

Arshad Ahmed
Partner
+1 574 236 7602
arshad.ahmed@crowe.com

Jaclyn Dettloff
Senior Manager
+1 818 325 8196
jaclyn.dettloff@crowe.com

Vikas Sharma
Senior Manager
+1 678 431 5411
vikas.sharma@crowe.com