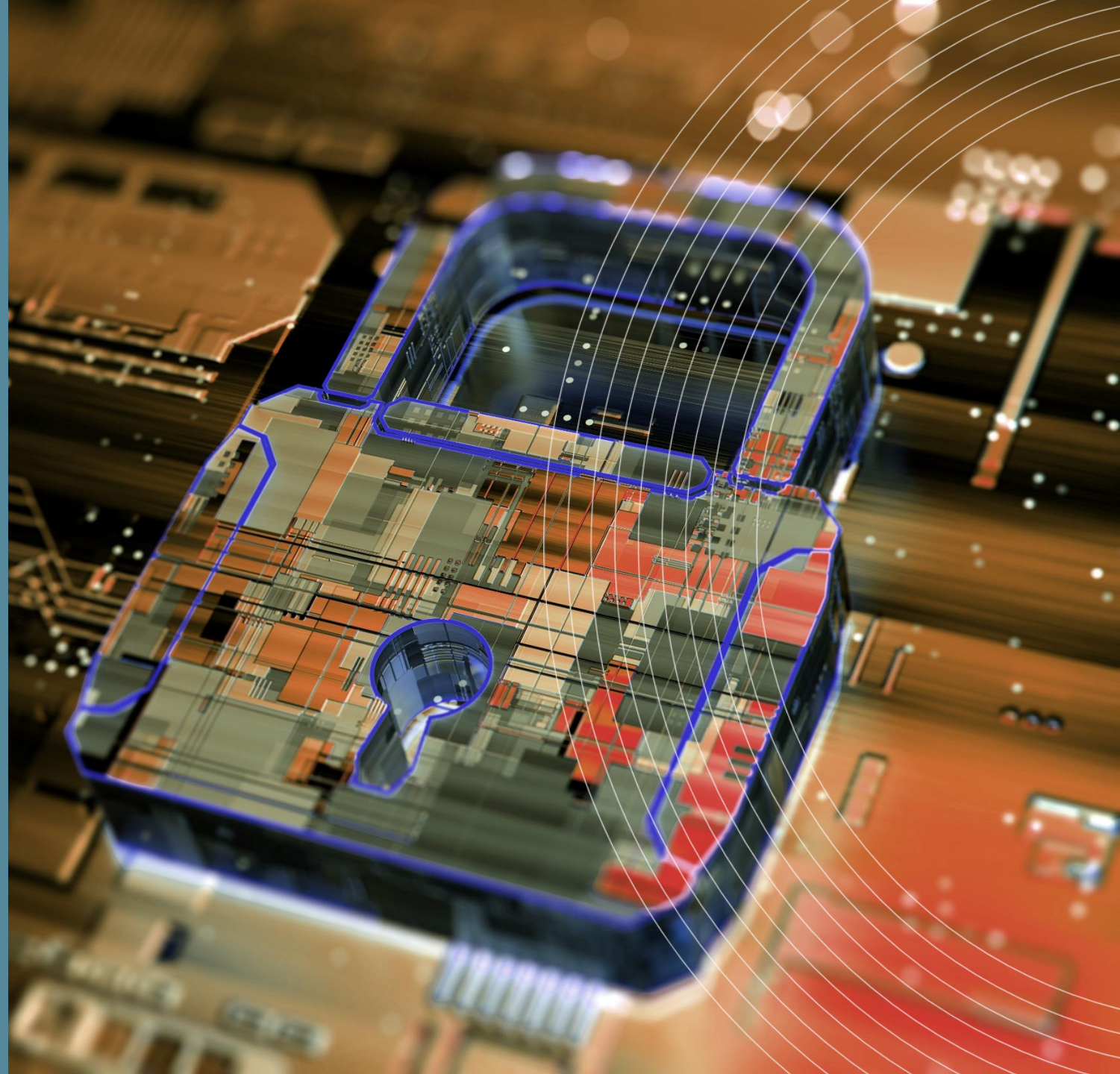
RISK ADVISORY SERVICES

Third-Party Risk Management:

SOC Reporting

HBK®



TODAY'S AGENDA

- Third-party Risk Management
- Introduction to SOC
- SOC 2
- Components of a SOC report
- How to use a report for your VRM?
- How to achieve SOC "Compliance"?

TODAY'S WEBINAR PRESENTERS

William J. Heaven, CPA, CISA, CITP, CSCP

Senior Manager, IT Department
HBK CPAs & Associates

Bill works out of the firm's corporate office in Youngstown, Ohio. He specializes in cyber security, IT security, external IT audit, internal IT audit, IT consulting, software development, IT governance, PCI-DSS, supply chain, system implementations and e-Commerce and has worked for a wide range of industries, including the Public Accounting field. Bill is a certified public accountant, a certified information system auditor, a certified information technology professional and a certified supply chain professional. He earned a bachelor's degree in Business Administration in Computer Science at Kent State University.

TODAY'S WEBINAR PRESENTERS

Matthew J. Schiavone, CPA, CISSP, CISA

Senior Manager, Risk Advisory Services
HBK CPAs & Associates

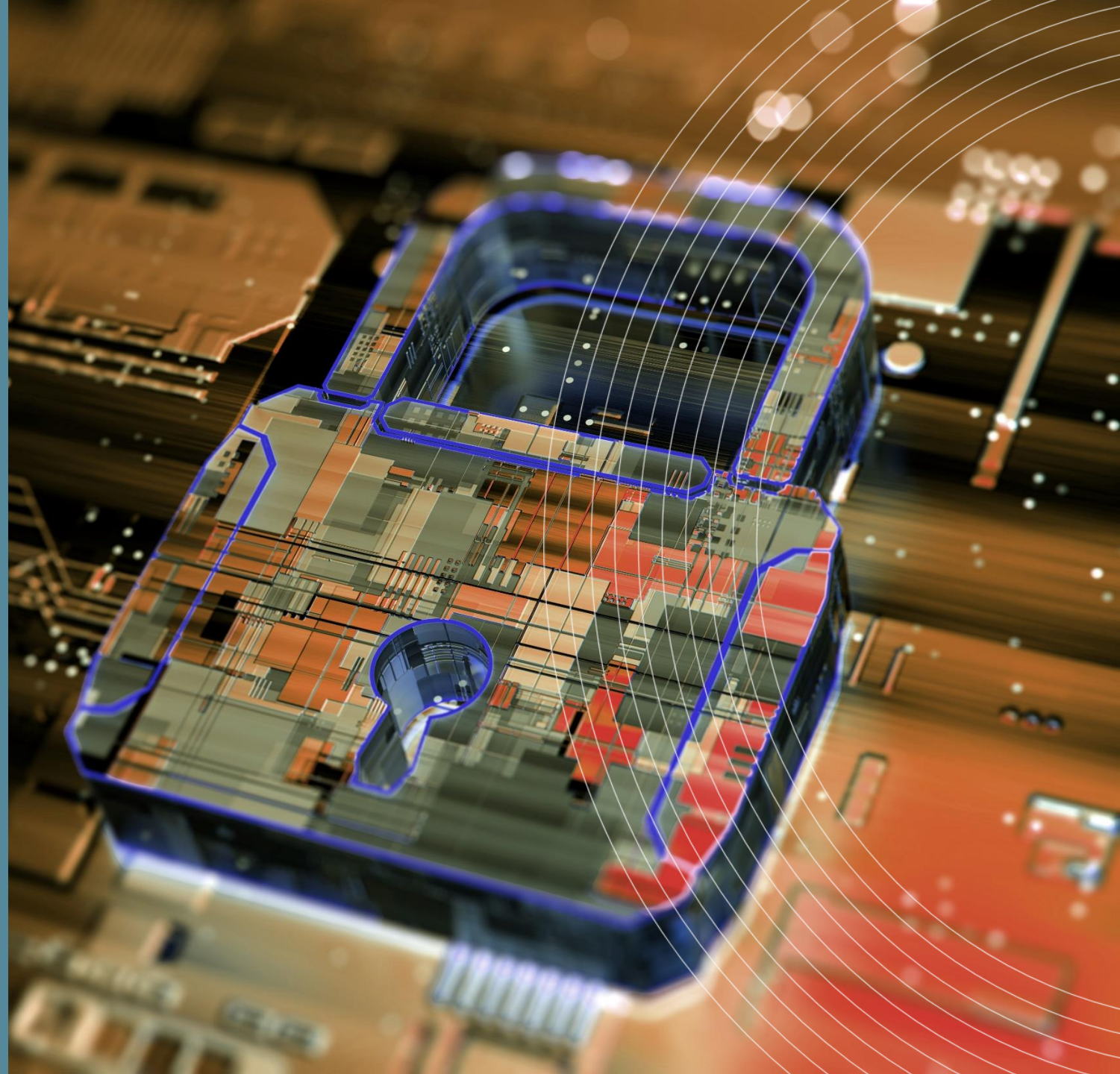
Matt is a Senior Manager in HBK's Quality Control department and works primarily in the Pittsburgh, Pennsylvania office. He specializes in risk advisory services, system and organization control (SOC) reporting, internal controls, IT audit, information security, and cyber security for all types of industries.

Matt is a certified public accountant, a certified information systems security professional, and a certified information system auditor. He earned a bachelor's degree in Accounting from Washington and Jefferson College.

RISK ADVISORY SERVICES

Third- Party Risk Management

HBK®



Third-Party Risk Management

Assessing your Third-Party Service Providers

- Process of analyzing and controlling risks associated with outsourcing third-party vendors/ service providers.
  - Example: Payroll, Data Centers, SaaS
- Vet providers before contracting and periodically thereafter
- 80% of organizations have had a breach that was caused by one of their vendors*

* 2020 Opinion Matters study https://www.bluevoyant.com/ciso-report-download-form

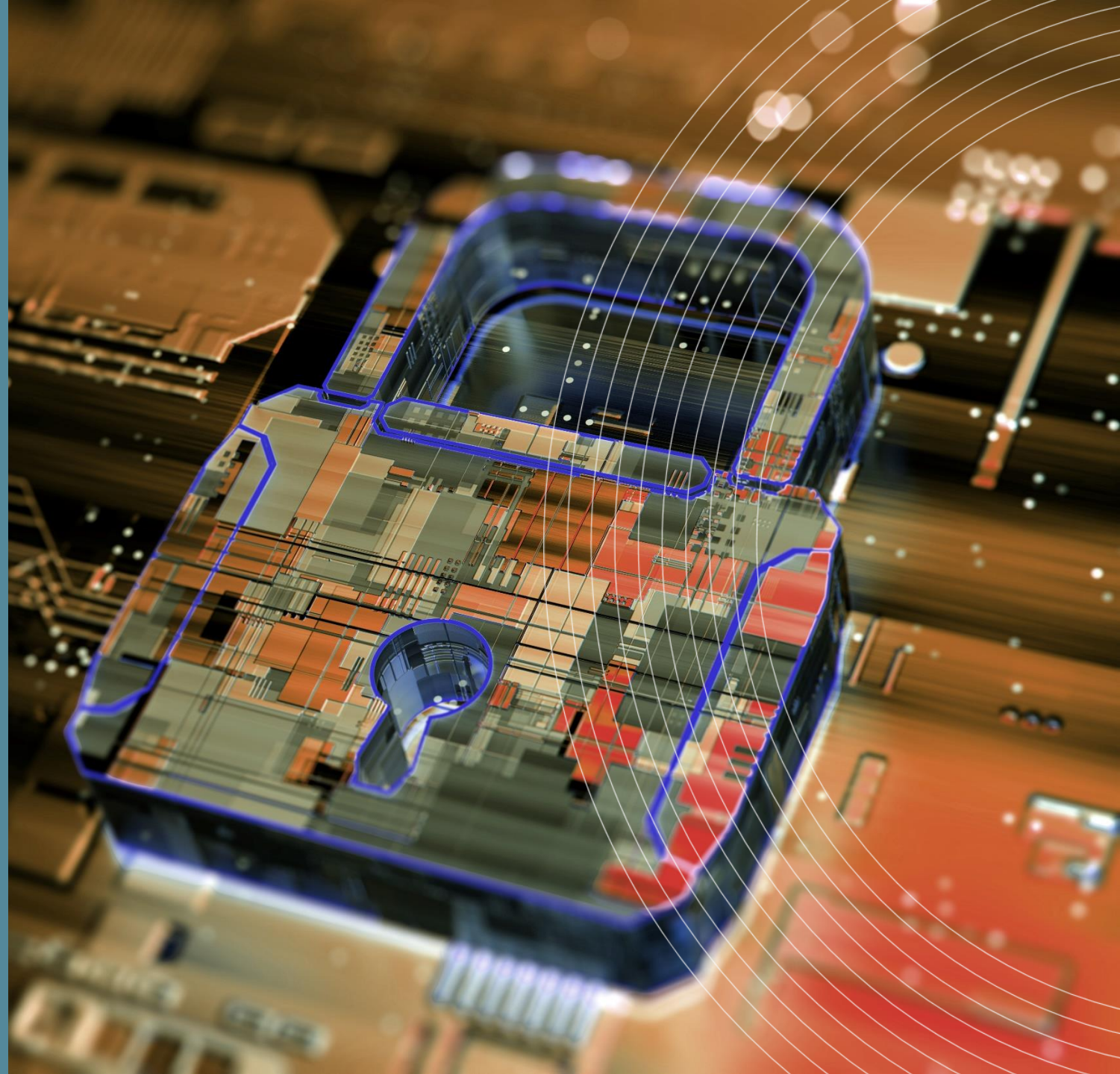
Third-Party Risk Management

Assessing your Third-Party Service Providers

- Vendor questionnaires and audit
- ISO 27001 Certification
- SOC Reports

RISK ADVISORY SERVICES

Introduction to SOC



HBK®

Introduction to SOC

Key Terms

- **Service organization**: an entity that possesses, stores, or handles information or transactions on behalf of its customers (user entities)
- **User entity**: the company that outsources its information or business processes to a service organization
- **Service auditor**: a CPA who reports on the controls of a service organization
- **User auditor**: a CPA who audits a user entity (often the financial statements)

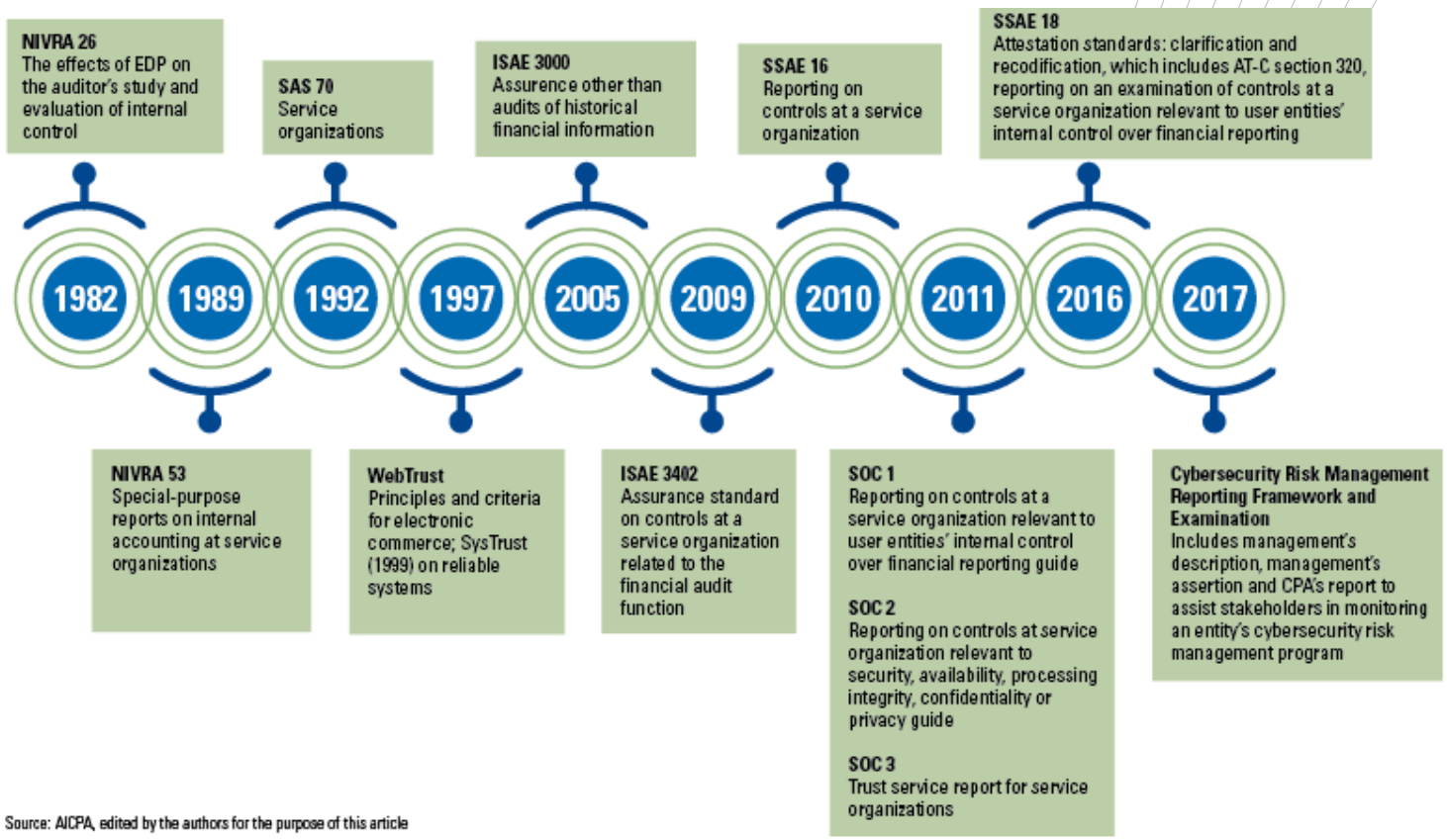
Introduction to SOC

What is SOC?

- System and Organization Control Reports
- Audit to provide assurance over service commitments
- Services offered by CPAs

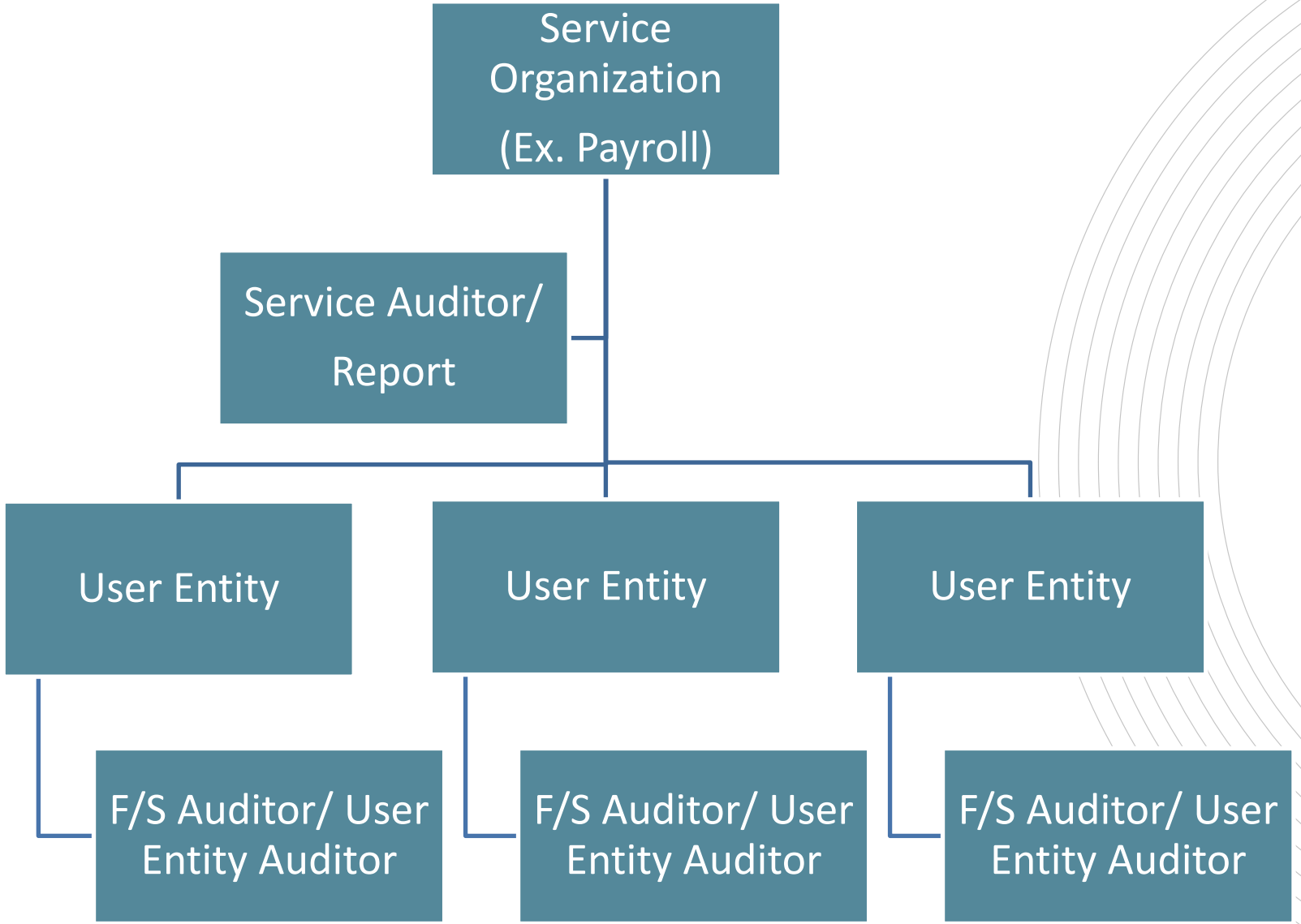
Introduction to SOC

Why CPAs?



Source: AICPA, edited by the authors for the purpose of this article

HBK®


Service Organization (Ex. Payroll)
Service Auditor/ Report
User Entity
User Entity
User Entity
F/S Auditor/ User Entity Auditor
F/S Auditor/ User Entity Auditor
F/S Auditor/ User Entity Auditor

Introduction to SOC

Benefits of undergoing SOC Examination

- reduce compliance costs and time spent on audits and filling out vendor questionnaires
- meet contractual obligations and marketplace concerns through flexible, customized reporting
- proactively address risks across your organization
- increase trust and transparency to internal and external stakeholders
- enhance reputation, credibility, marketability

Introduction to SOC

Types of SOC Examinations

- **SOC 1:** *Internal Controls over Financial reporting*
- **SOC 2:** *Trust Service Criteria*
- **SOC 3:** *Trust Service Criteria General Use Report*
- **SOC for Cybersecurity*:** *Cyber Risk Management Program*
- **SOC for Supply Chain*:** *System for Producing, manufacturing, or distribution*

*NEW

	What it reports on	Purpose	Who uses it
SOC 1	Internal controls over financial reporting relevant to a users' financial reporting	Reports on controls for Financial Statement Audits	User auditors, users' controller's office, upper management
SOC 2	Controls over security, availability, processing integrity, confidentiality, or privacy	Reports on controls related to compliance or operations	Senior Management, regulators, and others
SOC 3	Controls over security, availability, processing integrity, confidentiality, or privacy	Reports on controls related to compliance or operations	Publicly available to anyone
SOC for Cybersecurity	Effectiveness of an organization's cybersecurity risk management program	Reports on controls related to compliance or operations	Customers, senior Management, Boards of Directors, investors, business partners,
SOC for Vendor Supply	Controls on a vendor's manufacturing processes	Reports on controls related to compliance or operations	Customers of manufacturers and distributors to better understand the security risk in their supply chains

Introduction to SOC

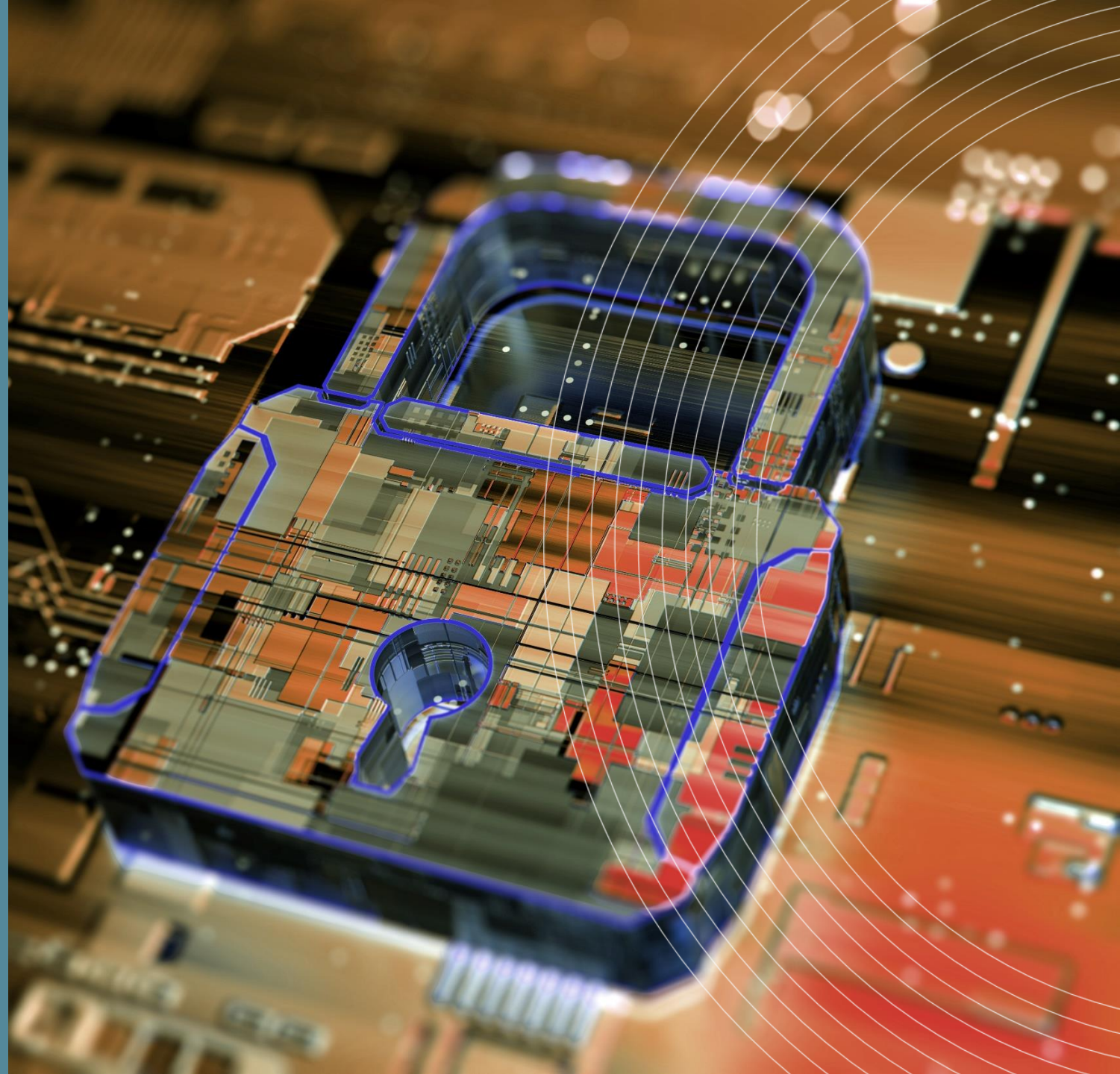
Types of Reports

- Type I: *Report on the design and implementation of controls*
- Type II: *Report on the design, implementation, and operating effectiveness of controls over a specified period*
- *Example: SOC 1 Type I; SOC 2 Type I; SOC 2 Type II*

RISK ADVISORY SERVICES

SOC 2

HBK®



SOC 2

Trust Service Criteria

- **Security**: The system is protected against unauthorized access (both physical and logical).
- **Availability**: The system is available for operation and use as committed or agreed.
- **Processing integrity**: System processing is complete, accurate, timely, and authorized.
- **Confidentiality**: Information designated as confidential is protected as committed or agreed.
- **Privacy**: Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and Chartered Accountants of Canada (CICA).

SOC 2

What are the Common Criteria?

- CC1.0: Organization and Management Controls
- CC2.0: Communication and Information
- CC3.0: Risk Assessment
- CC4.0: Monitoring
- CC5.0: Control Activities
- CC6.0: Logical and Physical Access
- CC7.0: System Monitoring
- CC8.0: Change Management
- CC9.0: Risk Mitigation

Introduction

CC1.0: Organization and Management Controls

- CC1.1 The entity demonstrates a commitment to integrity and ethical values.
- CC1.2 The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Introduction

CC2.0: Communication and Information

- CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
- CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.

Introduction

CC3.0: Risk Assessment

- CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- CC3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.
- CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.

Introduction

CC4.0: Monitoring

- CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.

Introduction

CC5.0: Control Activities

- CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.
- CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Introduction

CC6.0: Logical and Physical Access

- CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
- CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
- CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Introduction

CC6.0: Logical and Physical Access

- CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
- CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
- CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
- CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
- CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Introduction

CC7.0: System Monitoring

- CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
- CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
- CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Introduction

CC7.0: System Monitoring

- CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
- CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Introduction

CC8.0: Change Management

- CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Introduction

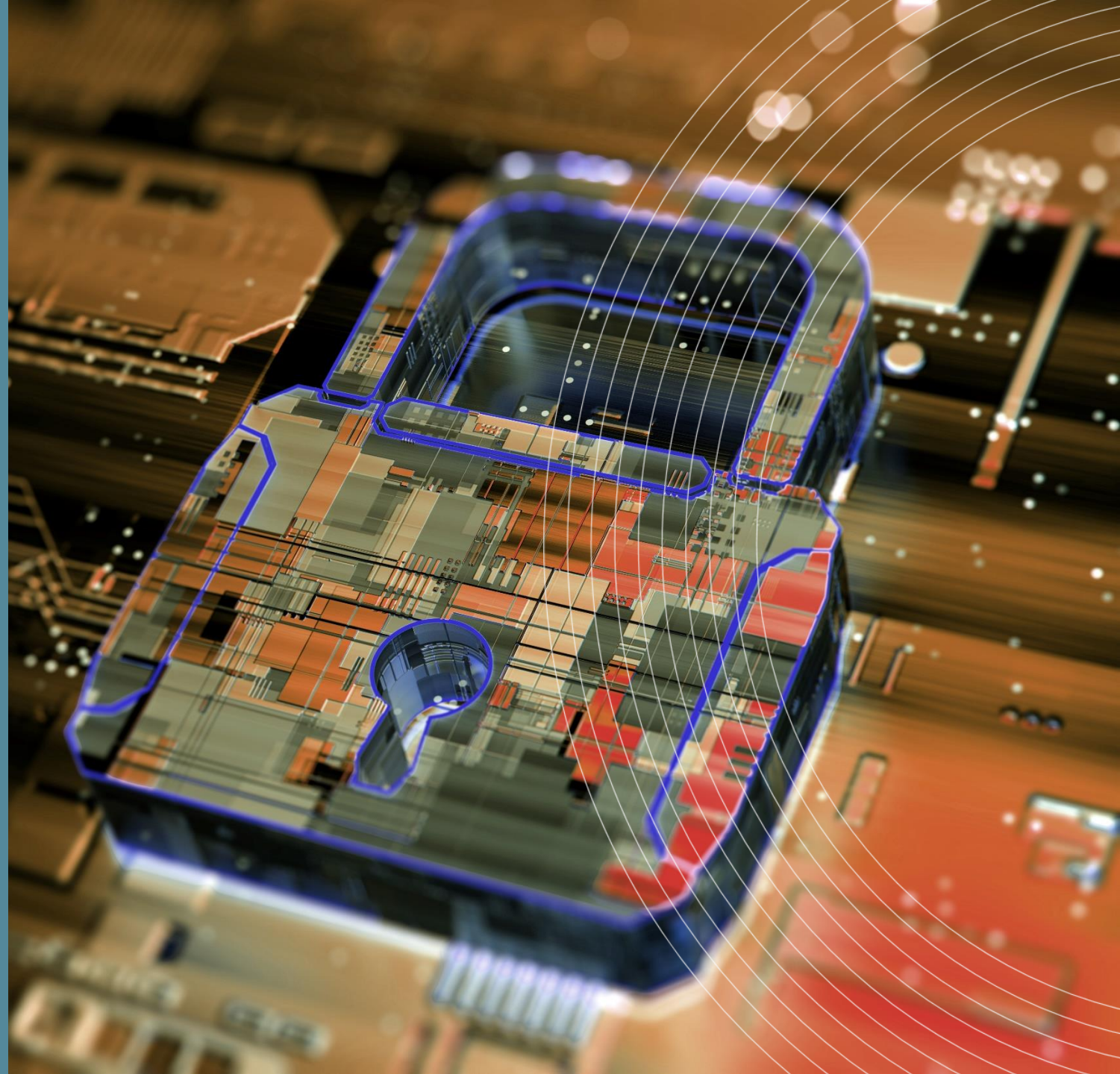
CC9.0: Risk Mitigation

- CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
- **CC9.2 The entity assesses and manages risks associated with vendors and business partners**.

RISK ADVISORY SERVICES

Components of a Report

HBK®



Components of Report

Section 1: Independent Auditor's Report

- Provides the reader the service auditor's opinion on the system description, design, and operating effectiveness to meet the control objectives

Components of Report

Section 2: Management Assertion

- Provides the reader the facts and assertions made by the service organization’s management related to the system(s) under audit

Components of Report

Section 3: Management's Description of System

- The detail of the system(s) being reported on (written by management)
- Boundary, infrastructure, controls, subservice organizations, user entity controls, and other system information
- Inclusions in this section should be capable of being audited to meet the control objectives

Components of Report

Section 4: Identified Controls and Tests of Controls

- Control objective (related to the applicable trust service principles)
- Controls in place at the service organization to meet the objectives
- Auditor's tests of the controls
- Results of the tests

Section 4: Identified Controls and Tests of Controls

Criteria	Criteria	Management Control	Test	Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A Business Continuity Plan has been developed to restore data and business operations in the event of a disruption.	Inspected Business Continuity Plan.	No exceptions noted.
		The Company has insurance to minimize the financial impact of any loss events.	Inspected evidence of insurance coverage.	Exception: The Company's insurance policy expired and was not renewed.

Components of Report

User Entity Controls

- Controls that the vendor has included within its system and rely on the user entity (you) to implement in order to achieve the vendor's control objectives.

Components of Report

Subservice Organization Controls

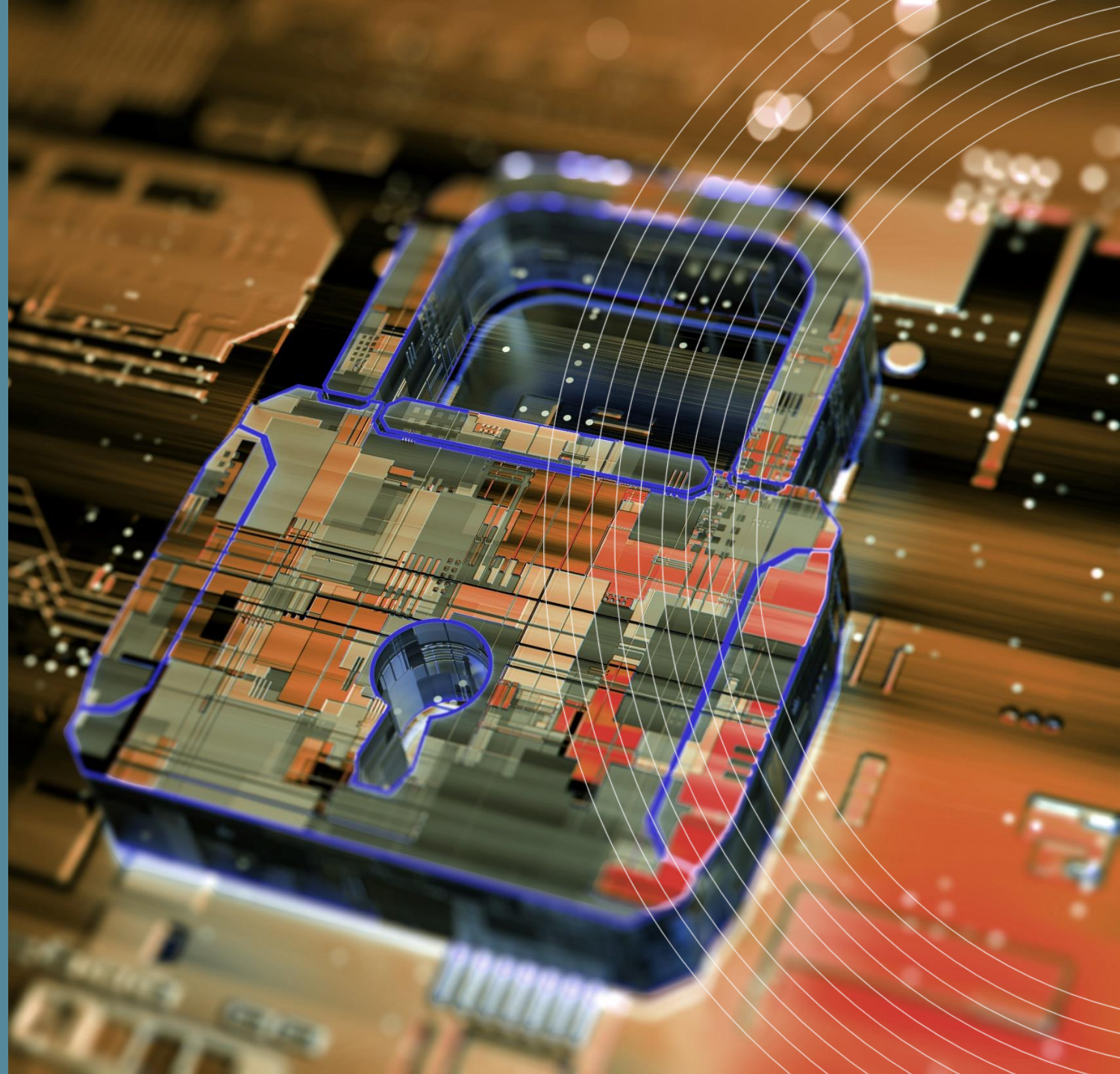
- Controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives

Components of Report

RISK ADVISORY SERVICES

Using Reports to Assess Third-party Risk

HBK®



Using the Report

Third-party Risk Management

Step 1: Identify your third-party service providers

Step 2: Request SOC Reports

Step 3: Review Section 1: Auditor's report.

- Does the scope cover the proper services?
- Time Period?
- Is it a Type I or Type II report?
- What is the auditor’s opinion?

Using the Report

Third-party Risk Management

Step 4: Review Identified Controls and Tests of Controls (Section IV)

- Are sufficient internal controls in place at the vendor?
- Are there any exceptions identified?
  - Do the exceptions introduce risk at your organization?

Step 5: Review User Entity Controls

- This section is important to review as it contains control considerations which the third party assumes are in place at your organization. Are they?

Using the Report

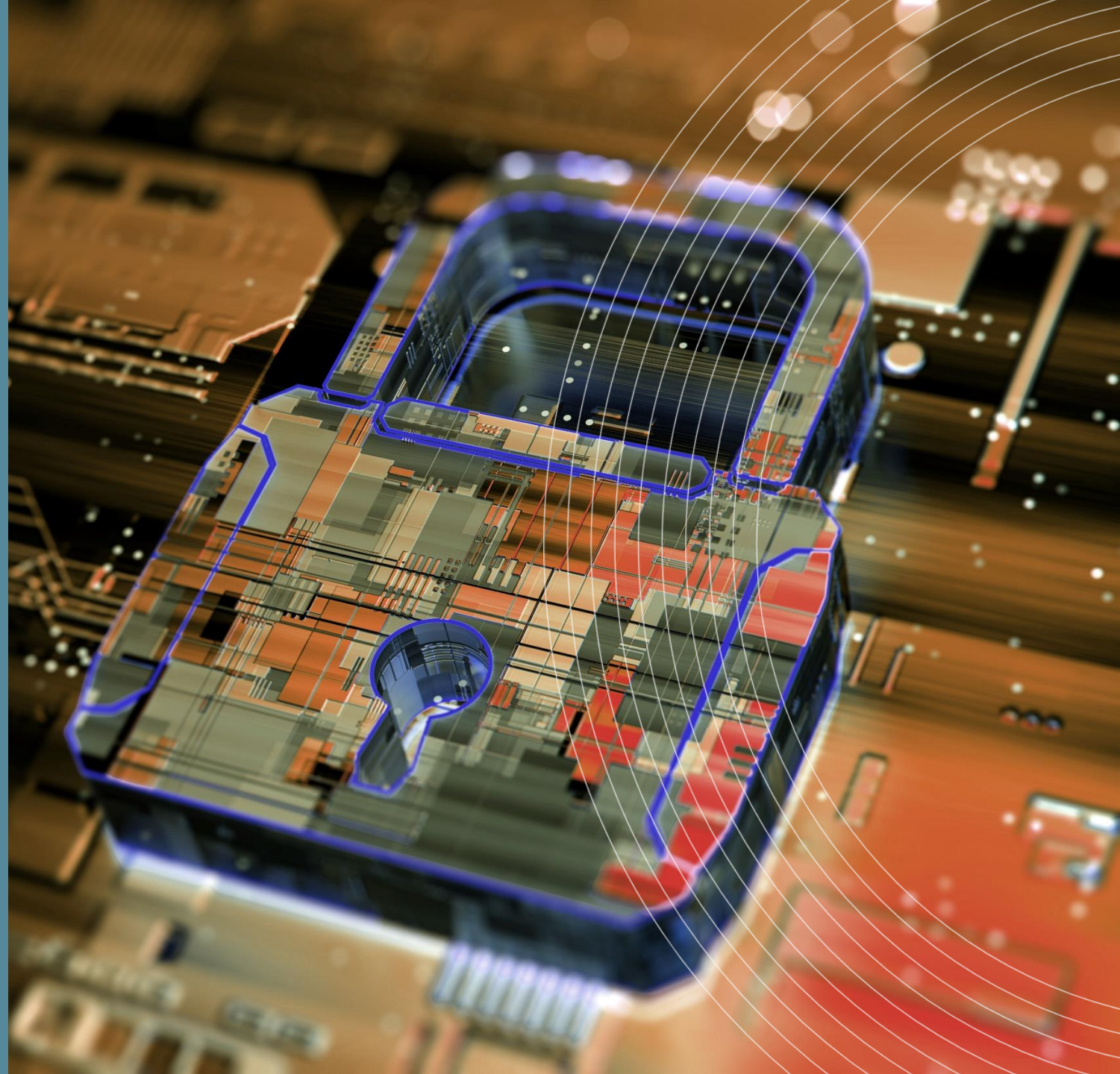
Misconceptions

- “Our vendor has a SOC report – that’s all we need to know!”
- “This is a report of the prior year activity, so it does us no good for present day and moving forward.”
- “Our vendor gave us their SOC report from two years ago and said nothing has changed—that’s good enough for us”
- “We only need to see a Type I report each year”

RISK ADVISORY SERVICES

Achieving SOC 2

HBK®



SOC Process

Readiness Assessment

- Identify Service Commitments, System Requirements, and System Boundaries
- Select Applicable Trust Service Criteria
- Conduct interviews, preform walkthroughs, and review policies to identify controls
- Map controls to TSC to identify gaps and weaknesses for remediation

SOC Process

Type I Reporting

- Test the implementation of controls
- Issue SOC 2 Type I report providing assurance the controls have been designed and implemented

SOC Process

Type II Reporting

- Return after a specified period
- Test the operating effectiveness of controls
  - Inspection of evidence throughout the period
  - Observe processes
  - Sampling

RISK ADVISORY SERVICES

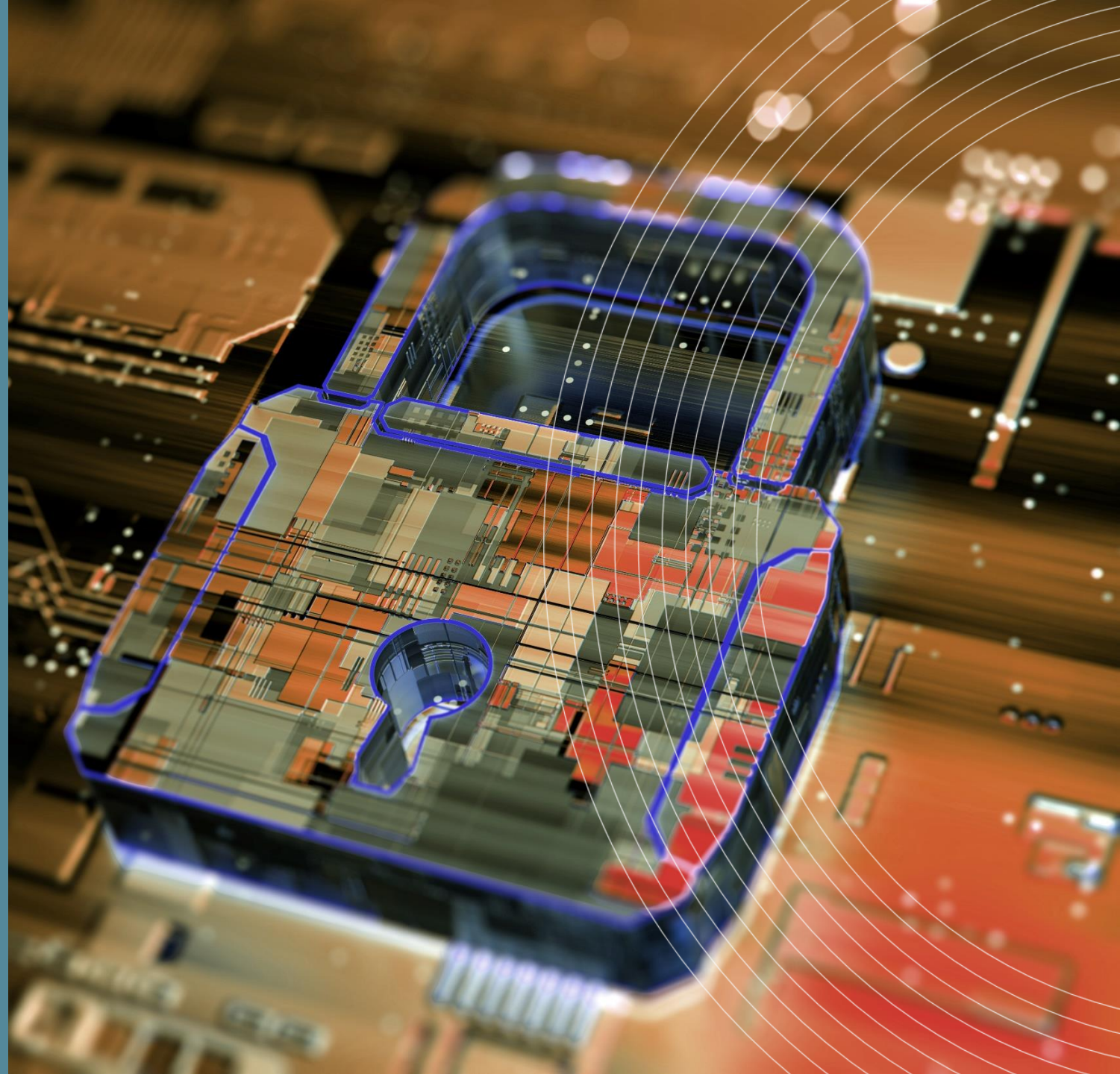
QUESTIONS?

Contact us.

Bill Heaven
HBK CPAs & Consultants
(330) 758-8613
wheaven@hbkcpa.com

Matt Schiavone
HBK CPAs & Consultants
(724) 934-5300
mschiavone@hbkcpa.com

HBK®



RISK ADVISORY SERVICES

THANK YOU FOR ATTENDING

HBK®