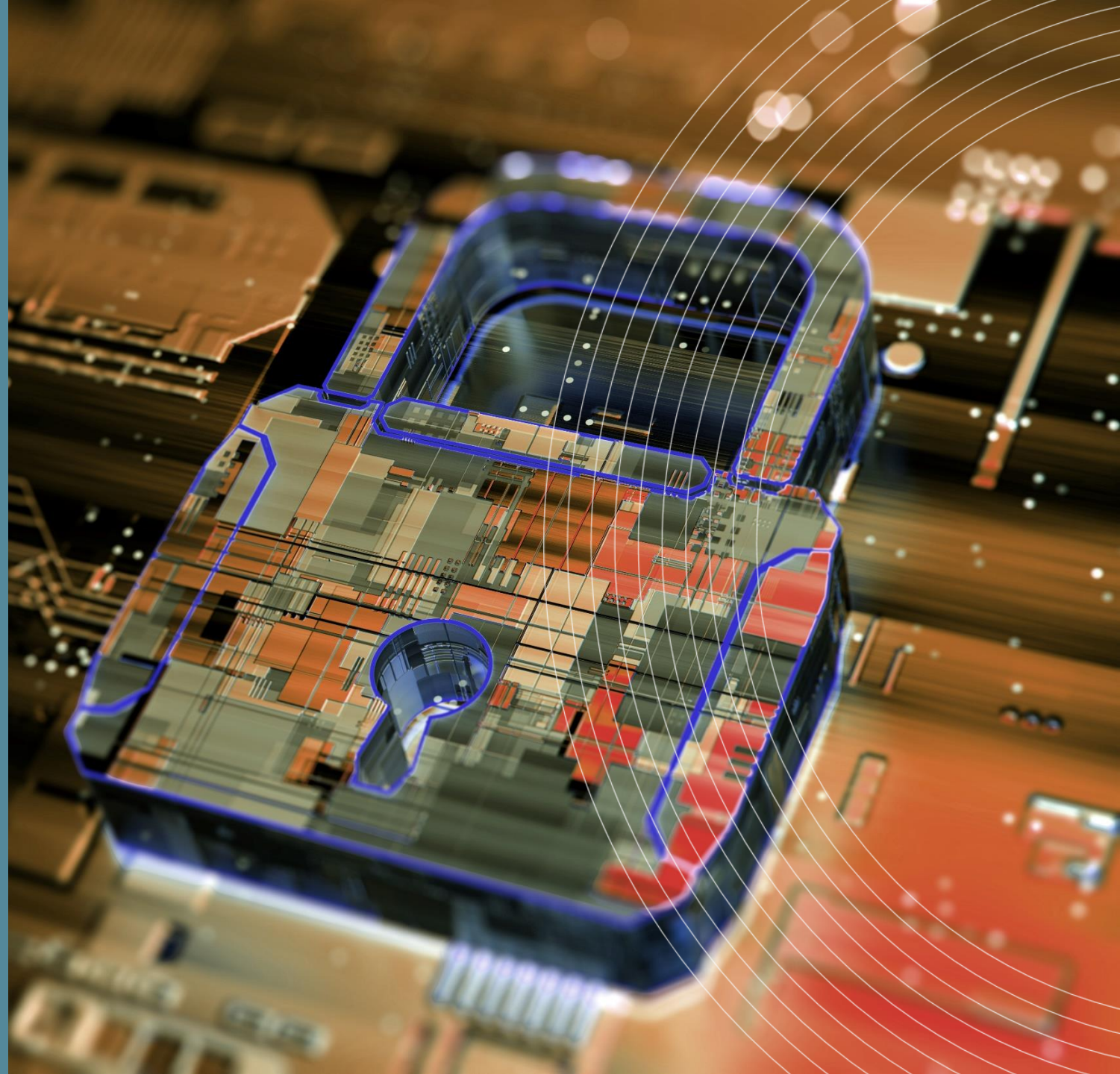
RISK ADVISORY SERVICES WEBINAR SERIES

How to Conduct an IT Risk Assessment

A Case Study

April 28, 2021

HBK®



Conducting a Risk Assessment

TODAY'S AGENDA

- Background
- Why Do You Need a Risk Assessment
- Risk Assessment Steps
- Wrap Up

TODAY'S WEBINAR PRESENTERS

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

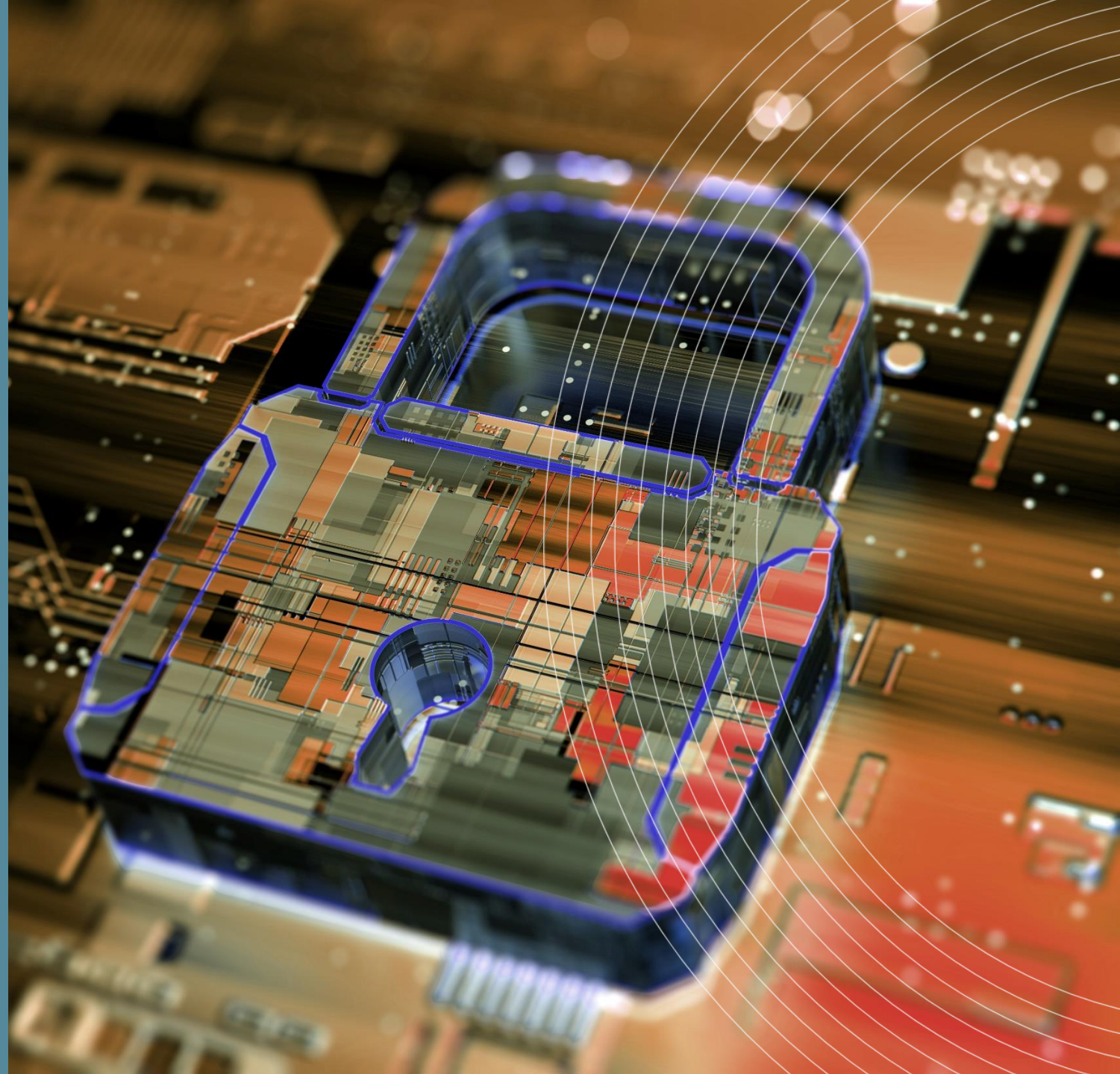
Matt is a certified public accountant, a certified information systems security professional, and a certified information system auditor. He earned a bachelor's degree in Accounting from Washington and Jefferson College.

RISK ADVISORY SERVICES WEBINAR SERIES

How to Conduct an IT Risk Assessment

Background

HBK®



Background

Key Terms and Definitions

- Risk
- Asset
- Threat
- Vulnerability
- Residual Risk
- Inherent Risk

Key Terms and Definitions

Risk

- The combination of the probability of an event and its consequence

Key Terms and Definitions

Asset

- Something of either tangible or intangible value that is worth protecting

Key Terms and Definitions

Threat

- Anything that is capable of acting against an asset in a manner that can result in harm

Key Terms and Definitions

Vulnerability

- A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Key Terms and Definitions

Residual Risk

- Remaining Risk after the implementation of a risk response

Key Terms and Definitions

Inherent Risk

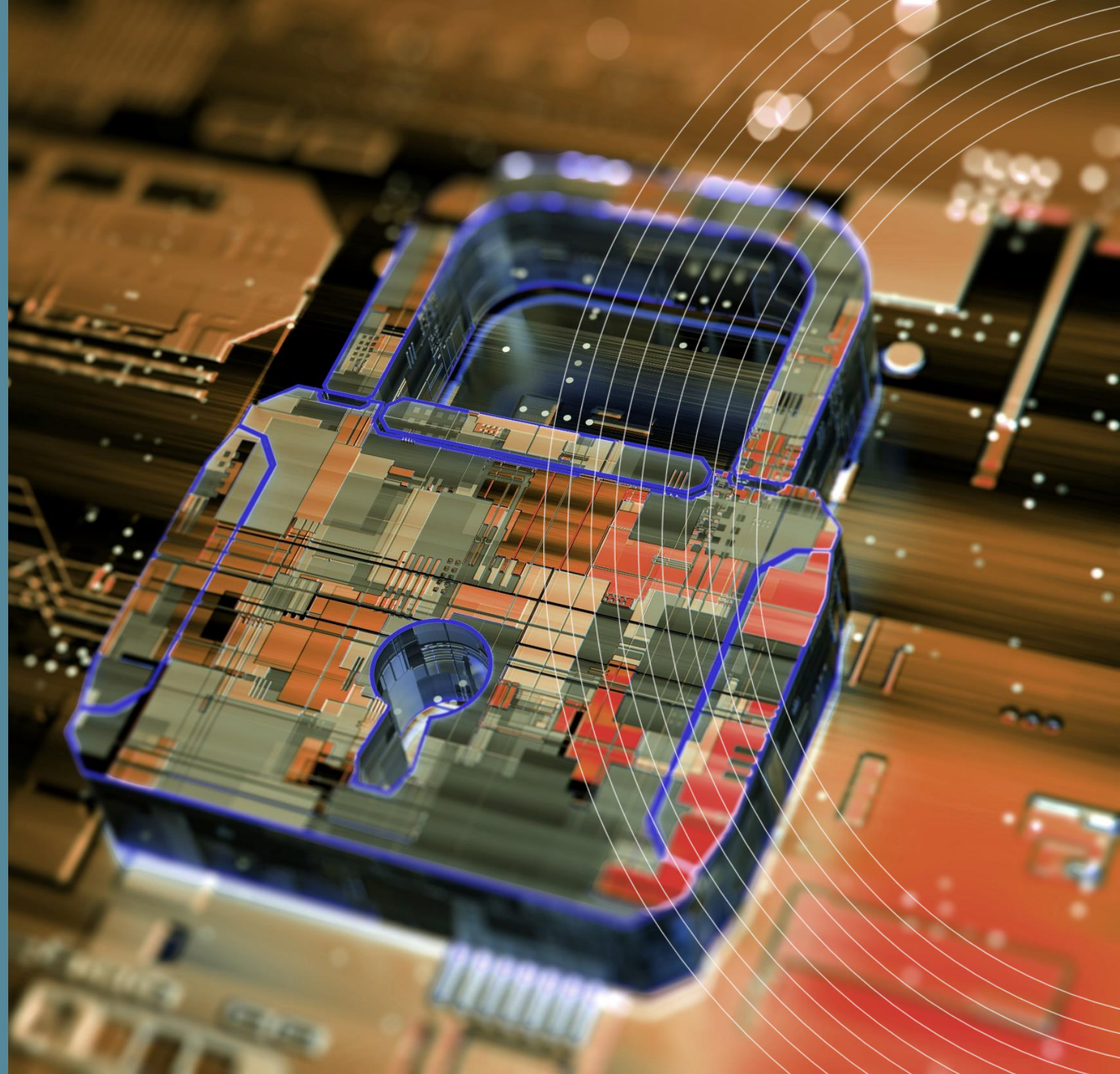
- The level of risk present without taking into account the actions that were or could be taken for mitigation

RISK ADVISORY SERVICES WEBINAR SERIES

How to Conduct an IT Risk Assessment

Why do you need a Risk Assessment?

HBK®



Should you perform a Risk Assessment?

Why?

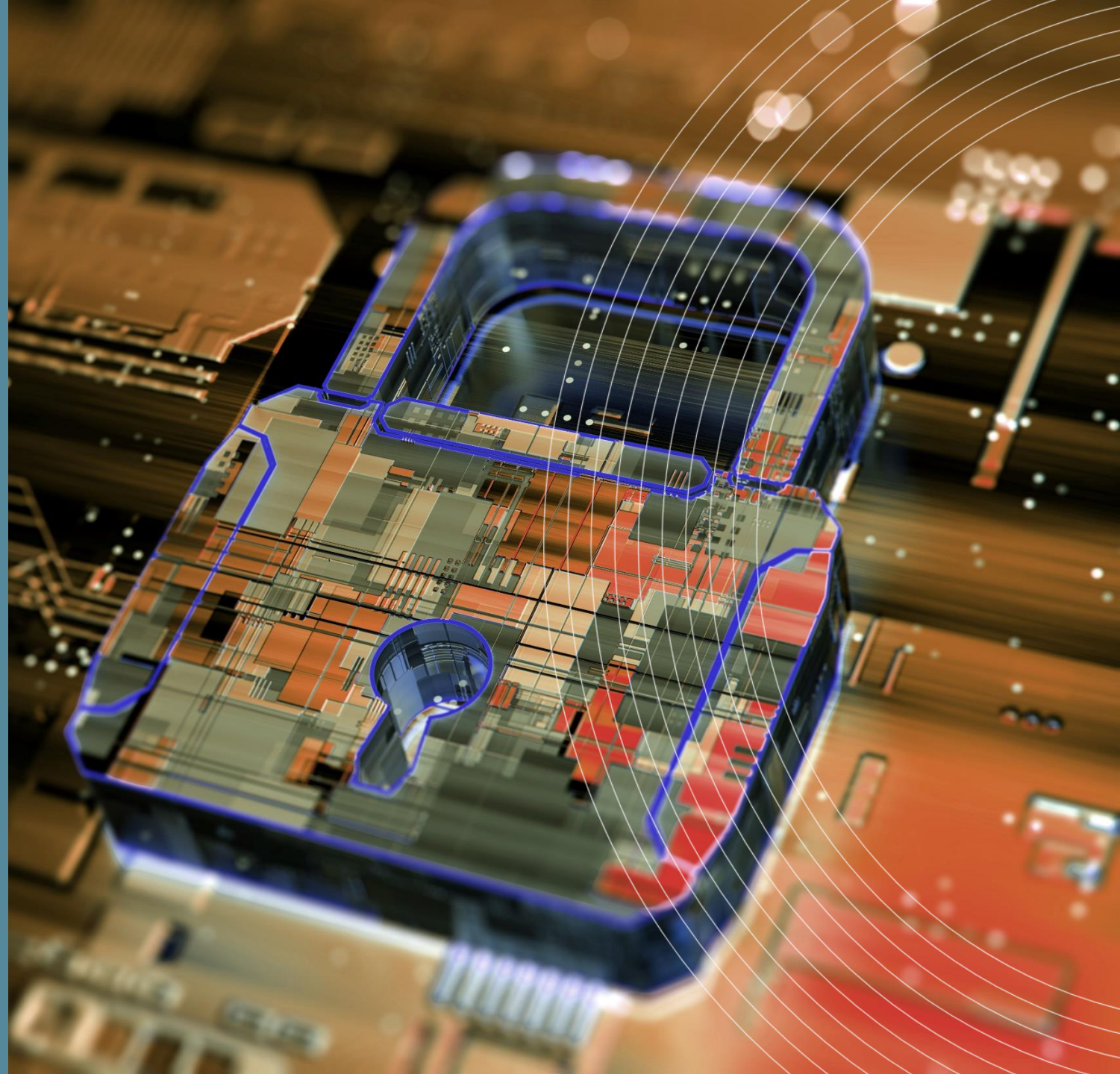
- Regulatory Requirement
- To Reduce Operational Risks
- To Improve Safety Performance
- To Improve the Probability of Achieving Organizational Objectives

RISK ADVISORY SERVICES WEBINAR SERIES

How to Conduct an IT Risk Assessment

Details / Steps

HBK®



Risk Assessment Details / Steps

1. Establish a Risk Assessment Framework
2. Identify Risks
3. Analyze Risks
4. Evaluate Risks
5. Apply Risk Management Options

Risk Assessment Details / Steps

Step 1

Establish a Risk Assessment Framework

- Conduct at regular Intervals
- Consistent and Repeatable Process
- Retain documentation regarding the process
  - Objective
  - Transparent
  - Auditable
- Baseline Security Criteria
- Determine your approach
  - Asset Based
  - Scenario Based

Asset Register

Asset	Asset Owner	Risk Owner
Desktop PC		
Laptop PC		
Printer		
Apple iPhone 10		
Apple iPad Pro		
Firewall		
Network Router		
Quick Books		
Windows 10		
Microsoft 365		

Risk Assessment Details / Steps

Step 2

Identify Risks

- Threats
- Vulnerabilities

Asset Register - continued

Asset	Asset Owner	Risk Owner	Threat	Vulnerability
Desktop PC			Ransomware	Inadequate level of Awareness / Knowledge of employees
Laptop PC			Unauthorized Access to Information Systems	Inadequate user rights/ permissions
Printer			Saved copies on internal storage	Information Disclosure
Apple iPhone 10			Lost or Stolen device	Unprotected device/ network access
Apple iPad Pro			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees
Firewall			Missed Security Patches	Kerberos Exploit
Network Router			Denial of Service Attack	Remote code execution
Quick Books			Powershell attack vector	Inadequate user rights
Windows 10			Easy to Guess Passwords	Inadequate level of Awareness / Knowledge of employees
Microsoft 365			Credential Theft	Lack of Security Training

Risk Assessment Details / Steps

Step 3

Analyze Risks

- Risk Appetite
- Risk Scale
- Risk Calculation
  - Risk = Impact x Likelihood

Asset Register - continued

Asset	Asset Owner	Risk Owner	Threat	Vulnerability	Impact (H/M/L)	Likeliness (H/M/L)	Risk (I x L)
Desktop PC			Ransomware	Inadequate level of Awareness / Knowledge of employees	3	3	9
Laptop PC			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6
Printer			Saved copies on internal storage	Information Disclosure	2	1	2
Apple iPhone 10			Lost or Stolen device	Unprotected device/ network access	3	1	3
Apple iPad Pro			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Firewall			Missed Security Patches	Kerberos Exploit	3	3	9
Network Router			Denial of Service Attack	Remote code execution	3	2	6
Quick Books			Powershell attack vector	Inadequate user rights	3	2	6
Windows 10			Easy to Guess Passwords	Inadequate level of Awareness / Knowledge of employees	3	3	9
Microsoft 365			Credential Theft	Lack of Security Training	3	3	9

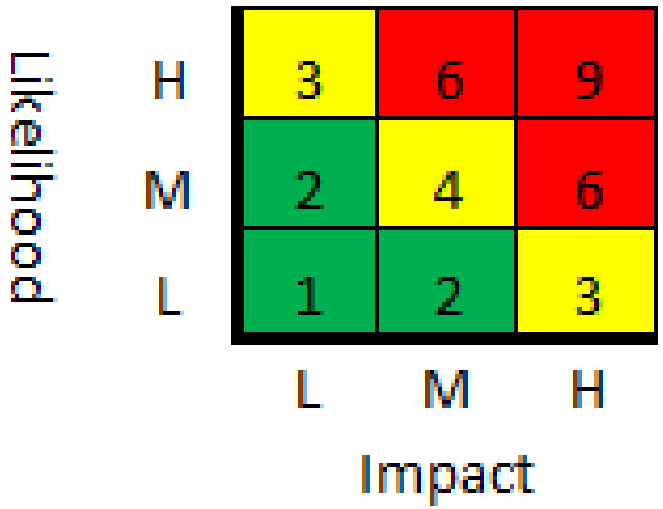
Risk Assessment Details / Steps

Step 4

Evaluate Risks

- Considerations
- Risk Matrix

Risk Matrix



Asset Register - continued

Asset	Asset Owner	Risk Owner	Threat	Vulnerability	Impact (H/M/L)	Likeliness (H/M/L)	Risk (I x L)	Controls
Desktop PC			Ransomware	Inadequate level of Awareness / Knowledge of employees	3	3	9	Security Awareness Training
Laptop PC			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6	IT Security Training / User Permissions / Security Log Monitoring
Printer			Saved copies on internal storage	Information Disclosure	2	1	2	IT Security Training / Asset Disposal Process
Apple iPhone 10			Lost or Stolen device	Unprotected device/ network access	3	1	3	Security Awareness Training / End Point Management
Apple iPad Pro			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6	Security Awareness Training / Security Log Monitoring
Firewall			Missed Security Patches	Kerberos Exploit	3	3	9	Vulnerability Management / Security Log Monitoring
Network Router			Denial of Service Attack	Remote code execution	3	2	6	Vulnerability Management / User Permissions
Quick Books			Powershell attack vector	Inadequate user rights	3	2	6	User Permissions / Security Log Monitoring
Windows 10			Easy to Guess Passwords	Inadequate level of Awareness / Knowledge of employees	3	3	9	Security Awareness Training
Microsoft 365			Credential Theft	Lack of Security Training	3	3	9	Security Awareness Training / Security Log Monitoring

Risk Assessment Details / Steps

Step 5

Apply Risk Management Options

- Risk Reduction
- Risk Avoidance
- Risk Transfer or Sharing
- Risk Acceptance

Risk Assessment Details / Steps

Risk Reduction

- The Implementation of controls or countermeasures to reduce the likelihood or impact of a risk to acceptable levels

Risk Assessment Details / Steps

Risk Avoidance

- Avoiding risk by not participating in an activity or business

Risk Assessment Details / Steps

Risk Transfer or Sharing

- Transferring risk to a third-party (i.e., insurance) or share with a third-party via contractual agreement

Risk Assessment Details / Steps

Risk Acceptance

- Assuming the risk and absorbing losses if the risk is within tolerance or the cost of mitigation exceeds the potential loss

How to Conduct an IT Risk Assessment

Next Steps

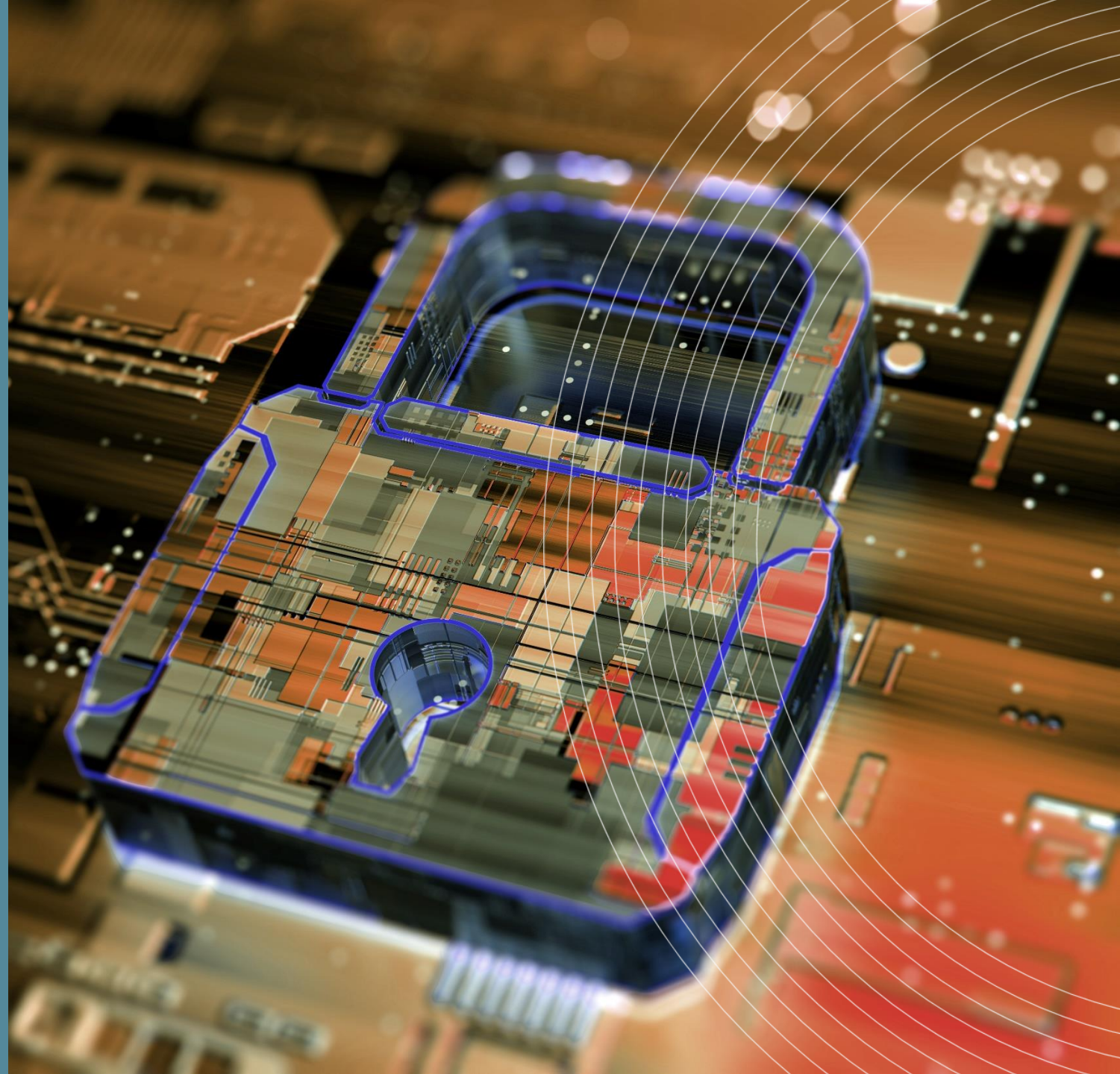
- Take Action
  - Risk Assessment Policy
  - Build your Asset Register (if approach)
  - Determine Threats and Vulnerabilities
  - Conduct your Risk Assessment
  - Risk Treatment Plan

RISK ADVISORY SERVICES WEBINAR SERIES

How to Conduct an IT Risk Assessment

Wrap Up

HBK®



How to Conduct an IT Risk Assessment

Wrap Up

- Background
- Why Do You Need a Risk Assessment
- Risk Assessment Steps

RISK ADVISORY SERVICES WEBINAR SERIES

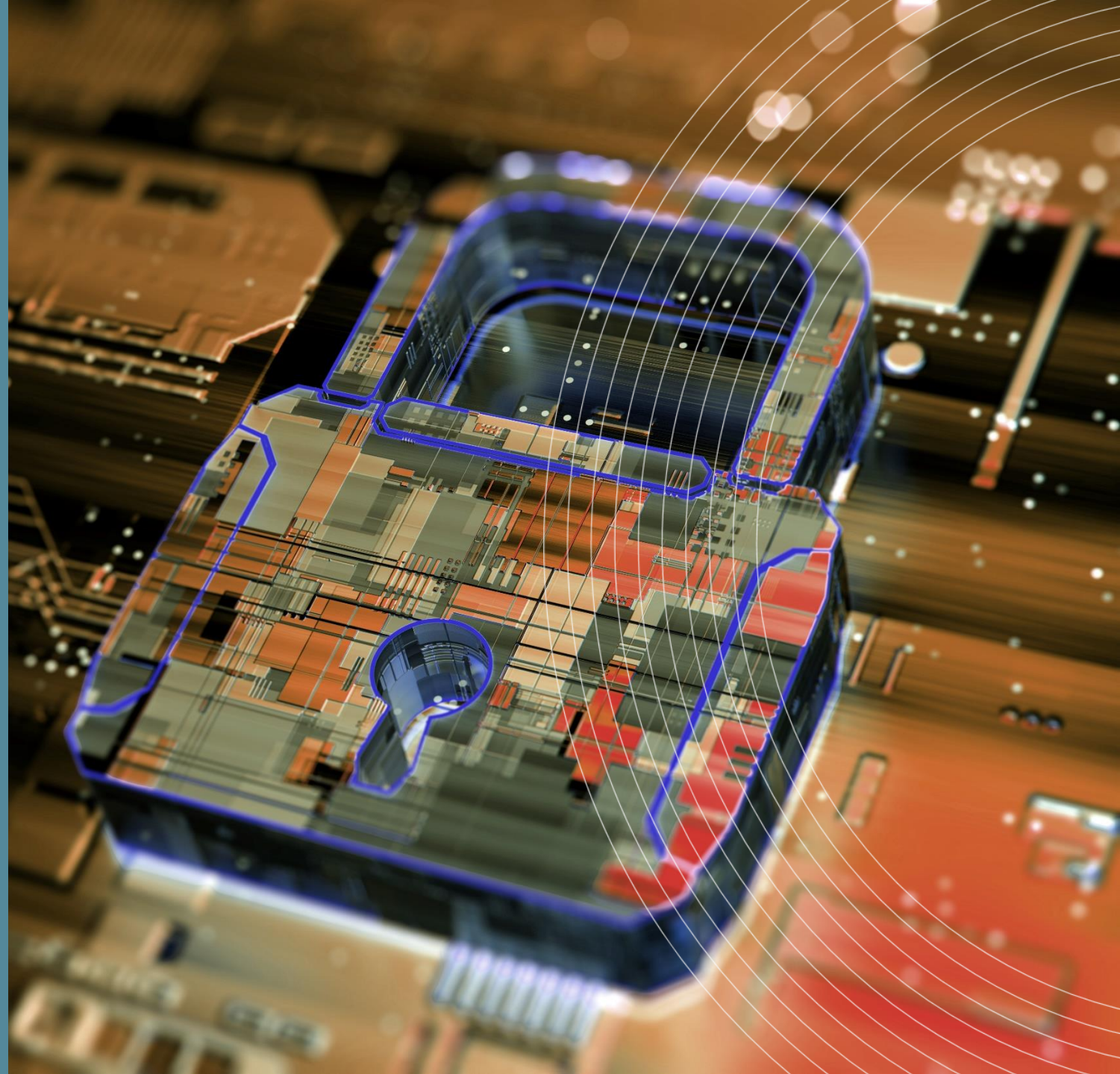
QUESTIONS?

Contact us.

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

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

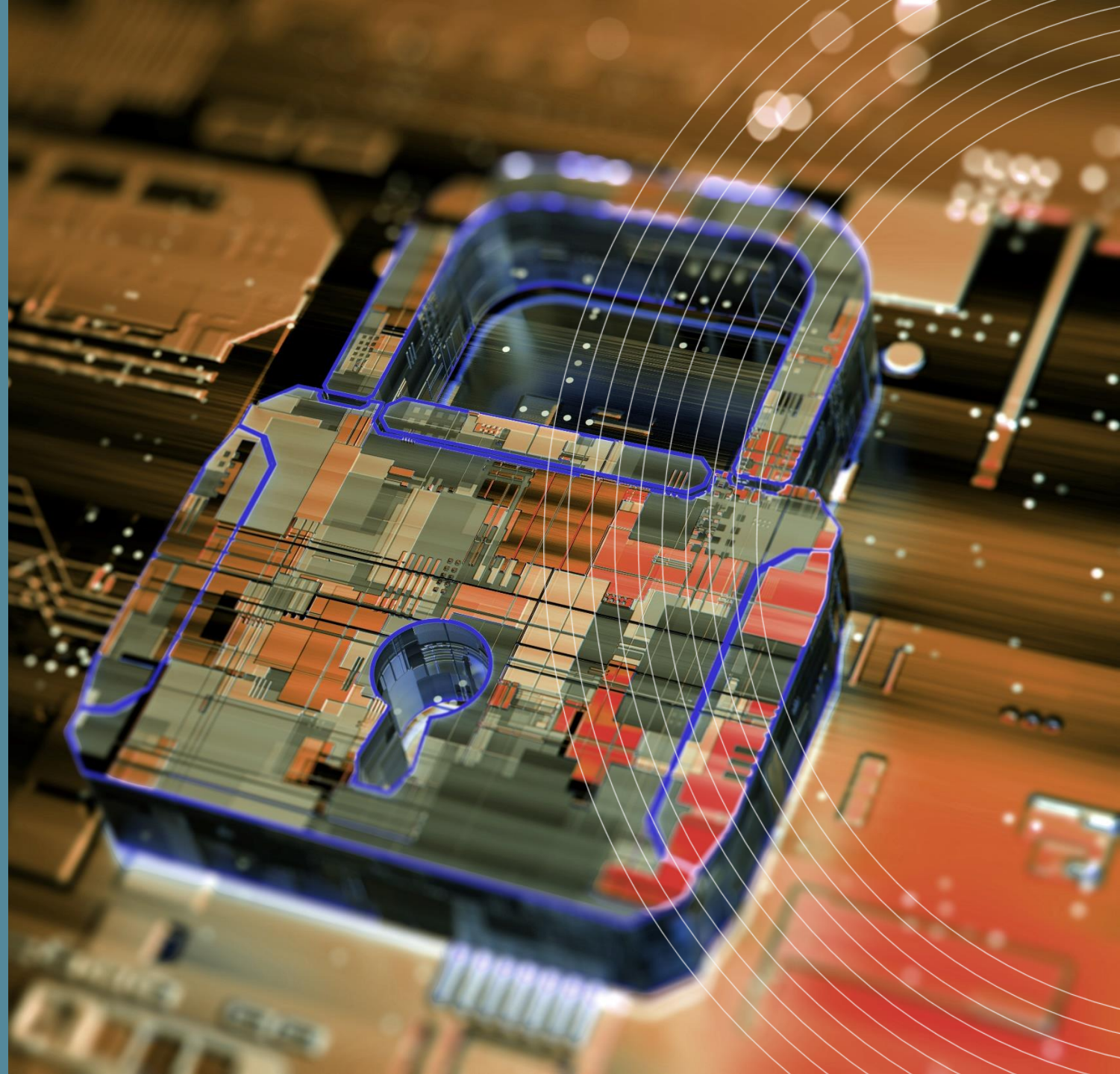
HBK®



RISK ADVISORY SERVICES WEBINAR SERIES

THANK YOU FOR ATTENDING

HBK®



Asset	Asset Owner	Risk Owner	Threat	Vulnerability	Impact (H/M/L)	Likeliness (H/M/L)	Risk (I x L)
Desktop PC			Ransomware	Inadequate level of Awareness / Knowledge of employees	3	3	9
Desktop PC			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6
Desktop PC			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Laptop PC			Lost or Stolen device	Unprotected device/ network access	3	1	3
Laptop PC			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6
Laptop PC			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Printer			Unauthorized changes to configuration settings	Privledge Escalation	2	2	4
Printer			Saved copies on internal storage	Information Disclosure	2	1	2
Printer			Internet access Attack Vector	Print Job Manipulation/ Information Disclosure	3	1	3
Apple iPhone 10			Lost or Stolen device	Unprotected device/ network access	3	1	3
Apple iPhone 10			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6
Apple iPhone 10			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Apple iPad Pro			Lost or Stolen device	Unprotected device/ network access	3	1	3
Apple iPad Pro			Unauthorized Access to Information Systems	Inadequate user rights/ permissions	3	2	6
Apple iPad Pro			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Firewall			Configuration Error	Weak Password / Inadequate user rights / Credential Theft	3	2	6
Firewall			Distributed Denial of Service Attack	VPN Vulnerability	3	2	6
Firewall			Missed Security Patches	Kerberos Exploit	3	3	9
Network Switch			Configuration Error	Weak Password / Inadequate user rights / Credential Theft	3	2	6
Network Switch			Phishing / Virus / Malware	Authentication Bypass	3	2	6
Network Switch			Denial of Service Attack	Remote code execution	3	2	6
Network Router			Configuration Error	Weak Password / Inadequate user rights / Credential Theft	3	2	6
Network Router			Router Table Poisoning Attack	Unauthenticated command injection	2	1	2
Network Router			Denial of Service Attack	Remote code execution	3	2	6

Quick Books			Powershell attack vector	Inadequate user rights	3	2	6
Quick Books			Configuration Error	Weak Password / Inadequate user rights / Credential Theft	3	2	6
Quick Books			Ransomware	Inadequate level of Awareness / Knowledge of employees	3	3	9
Windows 10			Configuration Error	Weak Password / Inadequate user rights / Credential Theft	3	2	6
Windows 10			Easy to Guess Passwords	Inadequate level of Awareness / Knowledge of employees	3	3	9
Windows 10			Phishing / Virus / Malware	Inadequate level of Awareness / Knowledge of employees	3	2	6
Microsoft 365			Credential Theft	Lack of Security Training	3	3	9
Microsoft 365			Out of date software / missed patches	Java Script / Web Page Vulnerability	3	3	9
Microsoft 365			Configuration vulnerabilities	Weak Password / Inadequate user rights / Credential Theft	3	2	6

Controls
Security Awareness Training
IT Security Training / User Permissions / Security Log Monitoring
Security Awareness Training
Security Awareness Training / End Point Management
IT Security Training / User Permissions / Security Log Monitoring
Security Awareness Training / Security Log Monitoring
IT Security Training / Security Awareness Training
IT Security Training / Asset Disposal Process
Security Awareness Training / User Permissions / Security Log Monitoring
Security Awareness Training / End Point Management
IT Security Training / User Permissions / Security Log Monitoring
Security Awareness Training / Security Log Monitoring
Security Awareness Training / End Point Management
IT Security Training / User Permissions / Security Log Monitoring
Security Awareness Training / Security Log Monitoring
Security Awareness Training
Vulnerability Management / User Permissions / Security Log Monitoring
Vulnerability Management / Security Log Monitoring
User Training / User Permissions / Security Log Monitoring
Security Awareness Training
Vulnerability Management / Security Log Monitoring
Security Awareness Training / User Permissions
Vulnerability Management / User Permissions
Vulnerability Management / User Permissions

User Permissions / Security Log Monitoring
Security Awareness Training / Security Log Monitoring
Security Awareness Training
Security Awareness Training / User Permissions / Security Log Monitoring
Security Awareness Training
Security Awareness Training
Security Awareness Training / Security Log Monitoring
Vulnerability Management / Security Log Monitoring
Security Awareness Training / Vulnerability Management / Security Log Monitoring