



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

Third Party Risk Management: Collision of Compliance, Privacy, and Security

Dr. Lisa McKee Ph.D., CISA, CDPSE, CRISC

Dr. Lisa McKee, Ph.D., CISA, CDPSE, CRISC

NIST

PROUD
MEMBER OF
**Accredited Standards
Committee X9TM**
Financial Industry Standards

women in
CYBERSECURITY
WiCyS

AMERICAN
SECURITY
& PRIVACY
BELLEVUE
UNIVERSITY



RSAConference



ONE IN TECHTM
An ISACA Foundation



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

UAH
THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

UCCS
University of Colorado
Colorado Springs

BELLEVUE
UNIVERSITY

ISACA

Learning Objectives

- Third Party Risk Management Program
- Track and monitor risk with third parties
- Common gaps in Third Party Risk Management Programs
- Tips, tactics, and techniques to get leadership support



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



Supply Chain Trends



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



Gartner Prediction March 2023...

“Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.”



<https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022>





ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



\$4.45m



The US average cost of a breach in 2023.

IBM Cost of a Data Breach Report 2023





ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



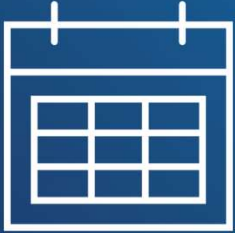
82%



Breaches involved data stored in the cloud.

IBM Cost of a Data Breach Report 2023





ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

307 Days

233 days to identify and 74 days to contain

IBM Cost of a Data Breach Report 2023





ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

Supply Chain Compromise

+12.8%

Time to Identify
Compromise

+11.8%

Compromise
Cost

IBM Cost of a Data Breach Report 2023



Notable Supply Chain Attacks

2020 – Solar Winds



<https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>

2021 – Kaseya

A massive ransomware attack hit hundreds of businesses. Here's what we know

By Clara Duffy, CNN Business
3 minute read · Updated 8:20 AM EDT, Wed July 7, 2021



<https://www.cnn.com/2021/07/06/tech/kaseya-a-ransomware-what-we-know/index.html>

2022 – Atlassian

Atlassian Confluence Questions app has a major security flaw... it uses a default password

Usama Jawad · Jul 21, 2022 05:16 EDT



<https://www.neowin.net/news/atlassian-confluence-questions-app-has-a-major-security-flaw-it-uses-a-default-password/>

2023 – Okta

Okta admits hackers accessed data on all customers during recent breach

Carly Page · @carlypage_ · 7:45 AM CDT · November 28, 2023



<https://techcrunch.com/2023/11/29/okta-admits-hackers-accessed-data-on-all-customers-during-recent-breach/>

2024 – Microsoft

US government review faults Microsoft for 'cascade' of errors that allowed Chinese hackers to breach senior US officials' emails

By Sean Lyngaas, CNN
3 minute read · Published 10:29 PM EDT, Tue April 2, 2024



<https://www.bleepingcomputer.com/news/security/microsoft-lazarus-hackers-breach-cyberlink-in-supply-chain-attack/>



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



Most Valuable Asset?



ISACA 2024
NORTH AMERICA
CONFERENCE



Data!

Robotics and Automation News July 2021....

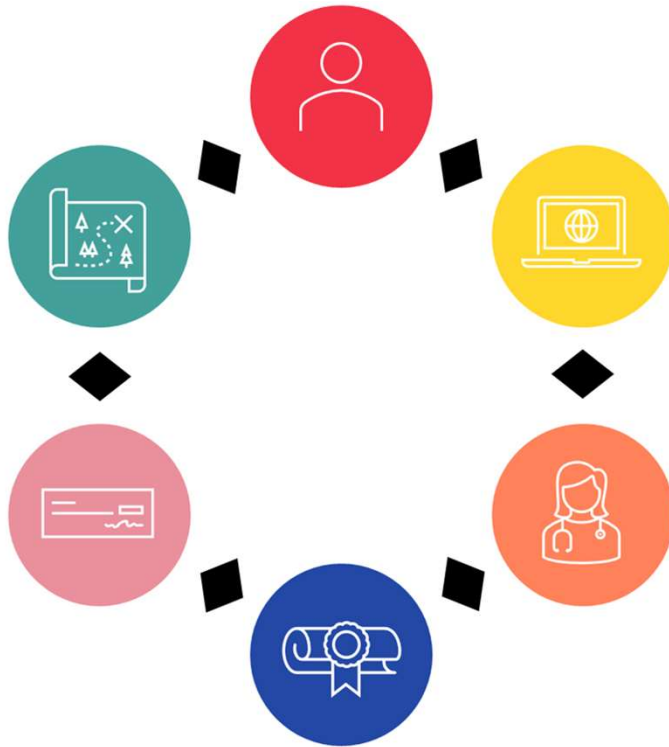
“Data: The Most Valuable Commodity for Businesses. The wider world of cyber could achieve a cumulative market value of \$280 billion by 2025, while data is now considered to be the globe’s most valuable and vulnerable resource.”



<https://roboticsandautomationnews.com/2021/07/22/how-has-data-become-the-worlds-most-valuable-commodity/44267/>



Categories of Personal Information



PI: Any information that can be linked to an identifiable individual

- Who You Are?
- Where Your Are?
- What Are You?

Why?



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

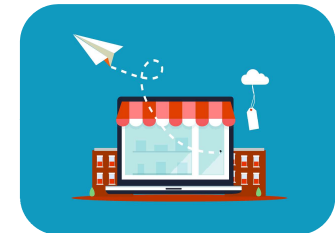
Money & Harm



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



- Company's make \$\$\$ on data aggregation and marketing
 - Targeted marketing
 - Sell to others
 - If you're not paying for a service, you're the product
- Adversaries want it too
 - Because they can
 - Money
 - Extortion

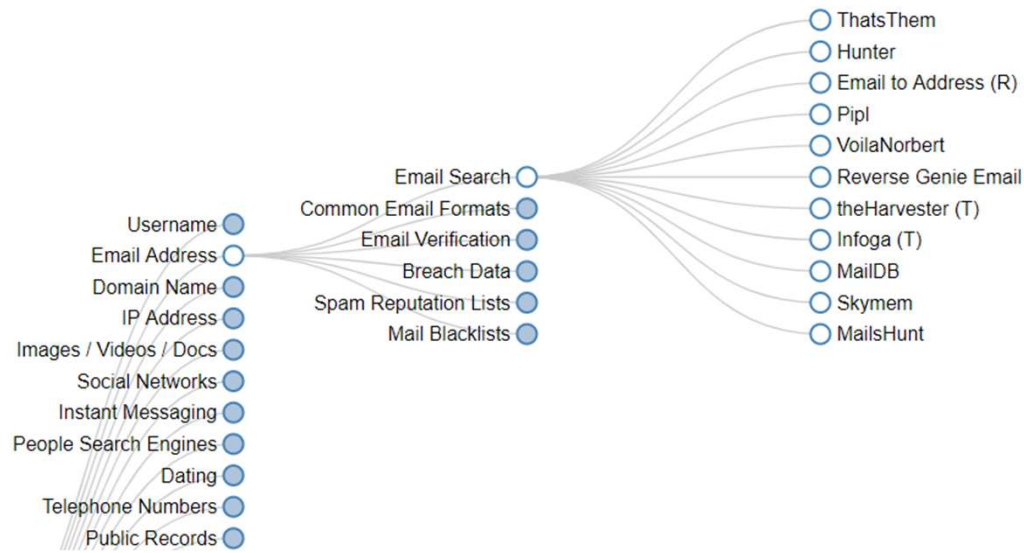


OSINT Framework



OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



<https://osintframework.com/>

MITRE ATT&CK Framework



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

MITRE | ATT&CK

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog Search

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (2)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (3)	Browser Session Hijacking	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (2)	Phishing (4)	Inter-Process Communication (2)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (2)	Create or Modify System Process (3)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (6)	Supply Chain Compromise (2)	Scheduled Task/Job (3)	Event Triggered Execution (14)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Multi-Factor Authentication Process (2)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Websites/Domains (2)		Trusted Relationship	Serverless Execution	Escape to Host	Domain or Tenant Policy Modification (2)	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	Event Triggered Execution (14)	Event Triggered Execution (14)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Impair Defenses (11)	Hide Artifacts (12)	Network Sniffing	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution (2)	Modify Authentication Process (2)	Impersonation	Hijack Execution Flow (12)	OS Credential Dumping (3)	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Indicator Removal (2)	Impair Defenses (11)	Steal Application Access Token	Log Enumeration		Email Collection (2)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings	Indirect Command Execution	Impersonation	Steal or Forge Authentication Certificates	Network Service Discovery		Input Capture (4)	Remote Access Software		
				Pre-OS Boot (3)	Masquerading (2)	Indirect Command Execution	Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Traffic Signaling (2)		
				Scheduled Task/Job (3)	Modify Authentication Process (2)	Masquerading (2)	Unsecured Credentials (3)	Peripheral Device Discovery		Video Capture	Web Service (2)		
				Server Software Component (3)	Modify Cloud Compute Infrastructure (3)	Modify Authentication Process (2)		Permission Groups Discovery (2)					
				Traffic Signaling (2)	Modify Registry	Modify Cloud Compute Infrastructure (3)		Process Discovery					
				Valid Accounts (4)	Modify System Image (2)	Modify Registry		Query Registry					
					Network Boundary Bridging (1)	Modify System Image (2)		Remote System Discovery					
					Obfuscated Files or Information (12)	Network Boundary Bridging (1)		Software Discovery (1)					
					Plist File Modification	Obfuscated Files or Information (12)		System Information Discovery					
					Pre-OS Boot (3)	Plist File Modification		System Location Discovery (1)					
					Process Injection (12)	Pre-OS Boot (3)		System Network Configuration Discovery (2)					
						Process Injection (12)		System Network Connections Discovery					

<https://attack.mitre.org/>

Core Privacy Rights



Access

- Free access to personal information that is collected on the consumer.
- Includes providing who else has access to the information.
- Must be prompt
 - US 45 days
 - EU 30 days
 - **Brazil 15 Days!**



Disclosure

- Provide privacy and data collection policies at or before time of collection.
- Disclose purpose of the information collection.
- Inform consumers of their rights under GDPR / CCPA.



Consent

- Consent must be obtained to market to the consumer (GDPR).
- Consumer can object to automated processing of data (GDPR).
- Consumer can opt out of having their information sold or transferred to other businesses or third parties (CCPA).



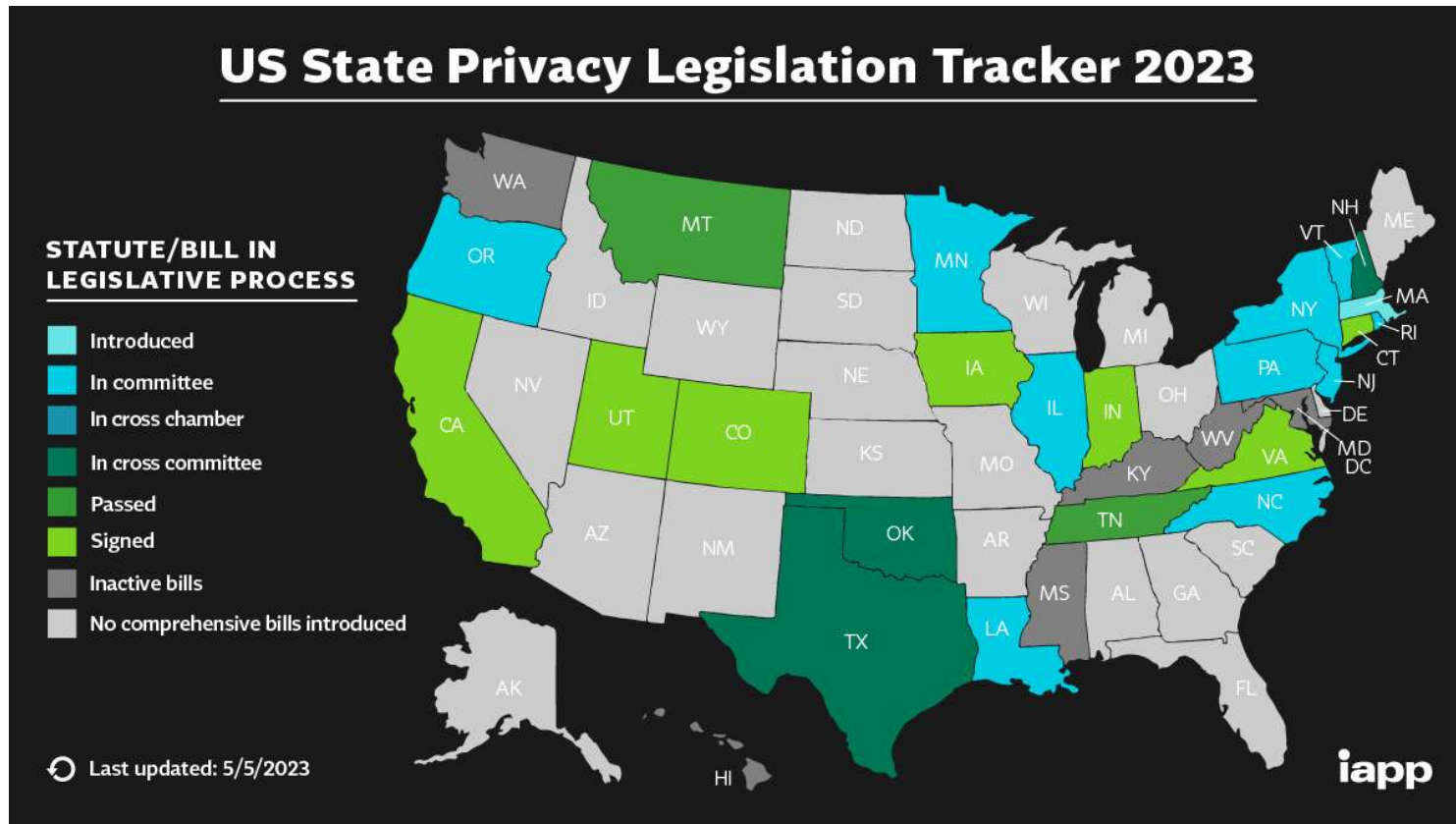
Deletion

- With certain exceptions, consumers have the right to have information about them deleted.
 - All data concerning the subject (GDPR).
 - All data collected from the consumer (CCPA).



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

A Year Ago - 7 State Privacy Regulations!

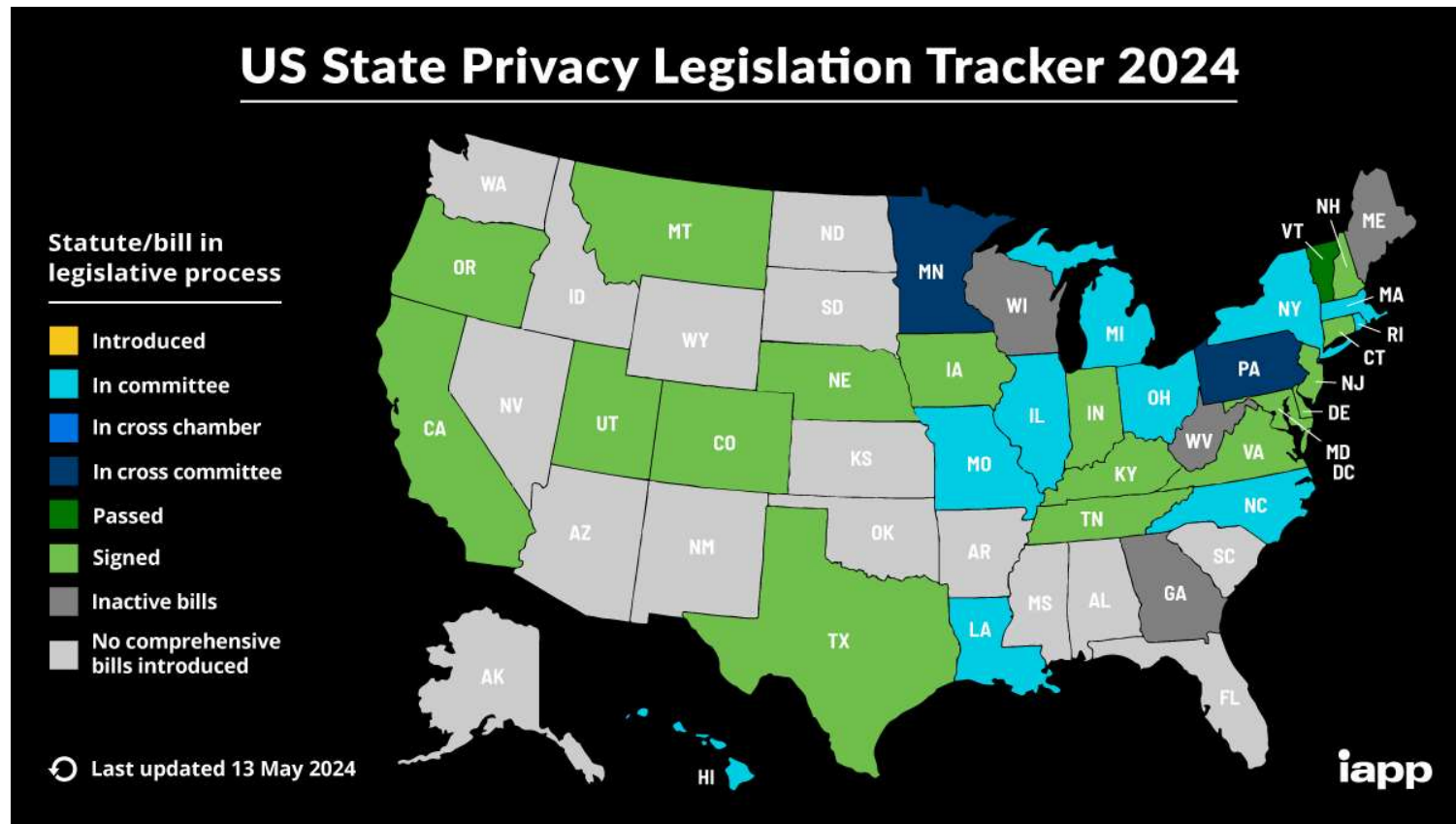


ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



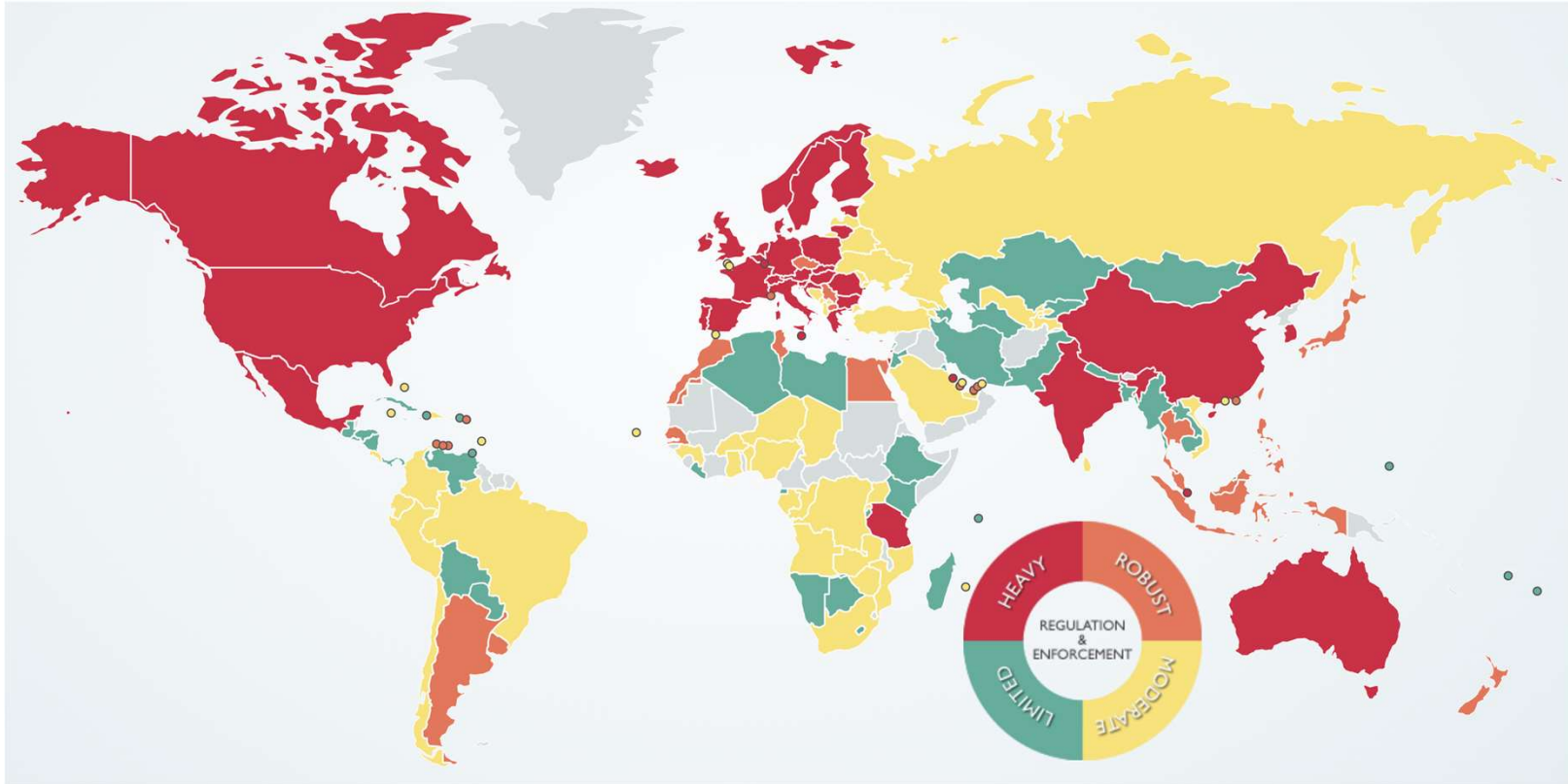
<https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#>

US Privacy Regulations – 17 Today!



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

International Privacy Regulations



<https://www.dlapiperdataprotection.com/>



Sample Organizational Compliance Footprint

Cybersecurity Laws

- Chinese Cyber Security (Nov 2018)
- New York Cybersecurity Regulation
- Ohio cybersecurity law 2018

Data Breach Laws

- Australia Data Breach Notification Law
- Federal Information Security and Data Breach Notification Laws
- Delaware Computer Security Breaches
- Hawaii Security Breach of Personal Information
- Indiana Disclosure of Security Breach
- Iowa Breach of Security Notification
- Kentucky Notification of Computer Security Breach
- Louisiana Database Security Breach Notification Law
- Massachusetts Security Breaches
- Minnesota Breach of Security
- Missouri Notice to Consumer for Breach of Security
- Montana Computer Security Breach
- New Hampshire Notice of Security Breach
- New Jersey Disclosure of Breach of Security to Customers
- New Mexico Data Breach Notification Act
- North Dakota Notice of Security Breach for Personal Information
- Pennsylvania Breach of Personal Information Notification Act
- South Carolina Breach of Security of Business Data
- Virginia Breach of Personal Information Notification
- Washington Personal Information Breach Notification
- West Virginia Breach of Security of Consumer Information
- Wyoming Computer Security Breach Notice to Affected Persons
- Guam Notification of Breach of Personal Information
- Virgin Islands Disclosure of Breach of Security

Financial Laws

- Consumer Financial Protection Act of 2010
- Federal Reserve Bank (FRB)
- Office of the Comptroller (OCC)
- Truth in Lending Act (TILA)

Government

- Federal Information Security Management Act (FISMA)
- Internal Revenue Service (IRS)

Healthcare Laws and Regulations

- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Trust Alliance (HITRUST)
- Virginia Breach of Medical Information Notification

Insurance

- South Carolina Department of Insurance Data Security Act 2018

International Data Privacy Laws

- Argentina Personal Data Transfer Restrictions 2018

- Asia-Pacific data Protection Law
- Australia Privacy Amendment Act 2017
- Austrian Data Protection Act 2018
- Bahrain Personal Data Protection Law 2018
- Belgium data protection 2017
- Brazil Data Protection Law
- Brussels

- Canada Personal Information Protection and Electronic Documents Act
- Canada Privacy Act
- Chile Data Protection Act
- China
- Columbia Data Protection Law (Jan 2017)
- Denmark
- Dubai International Financial Centre (DIFC)
- European Union Privacy
- EU Data Protection Act 2018
- European Union General Data Protection Regulation (EU GDPR)

- France
- French Data Protection Bill of 2018
- Finland
- Germany
- Greece
- Hong Kong
- India Personal Data Protection Bill (2018)
- Indonesia
- Ireland
- Italy (Sept 2018)
- Kenya
- Latin American Data Protection Law
- Law of the Republic of Armenia
- Luxembourg
- Malta
- Mexico
- Mozambique

- Norway
- Poland
- Portugal
- Privacy Shield EU-US
- Privacy Shield Swiss-US
- eIDAS PSD2
- Qatar
- Qatar Financial Centre
- Russian Federation
- Senegal
- Serbia
- Singapore
- South African Data Protection Act of 2018
- South Korea
- Spain
- Sweden
- Switzerland
- Taiwan
- Thailand
- Turkey
- UK Bribery Act 2010 (UK BA)
- UK Data Protection Act 2018
- UK (England and Wales)
- UK (Scotland)
- UK Secure by Design

- Vietnam Data Privacy (Jan 2019)

Other

- Export Administration Regulations (EAR)
 - Anti-Boycott Regulations (Part 760 of the EAR)

State Data Privacy Laws

- Alabama Deceptive Trade Practices Act
- Alaska Personal Information Protection Act
- Alaska Unfair Trade Practices and Consumer Protection Act
- Arkansas Deceptive Trade Practices Act
- California Consumer Privacy Act
- CalOPPA
- California Preservation and Regulation of Competition
- Colorado Consumer Protection Act (Sept 2018)
- Delaware Online Privacy and Protection Act
- Florida Security of Confidential Information\ Georgia Identify Theft
- Idaho Identify Theft
- Illinois Personal Information Protection Act
- Kansas Consumer Protection Act
- Kansas Protection of Consumer Information
- Kentucky Consumer Protection Act
- Maine Notice of Risk to Personal Data
- Maryland Personal Information Protection Act
- Massachusetts Regulations of Business Practice and Consumer Protection Act
- Massachusetts Standards for the Protection of Personal Information
- Michigan Identify Theft Protection Act
- Michigan Consumer Protection Act
- Minnesota Prevention of Consumer Protection Fraud Act
- Mississippi Consumer Protection Act
- Montana Consumer Protection Act
- Nebraska Consumer Protection Act
- Nevada Security of Personal Information
- North Carolina Identity Theft Protection Act
- Oregon Consumer Identity Theft Protection Act
- Rhode Island Identity Theft Protection Action of 2015
- Rhode Island Safe Destruction of Documents Containing Personal Information
- Tennessee Consumer Protection Act
- Texas Personal Identity Information
- Texas Identity Theft Enforcement and Protection Act
- Utah Protection of Personal Information Act
- Vermont Protection of Personal Information
- Wisconsin Notice of Unauthorized acquisition of Personal Information
- Guam Social Security Number Confidentiality Act
- Puerto Rico Citizen Information on Data Banks Security Act

US Corporate Laws and Regulations

- Equal Employment Opportunity Commission (EEOC)
 - Americans with Disabilities Act (ADA)
 - Age Discrimination in Employment Act (ADEA)
 - Equal Pay Act (EPA)

- Employee Retirement Income Security Act of 1974 (ERISA)
- Employee Retirement Income Security Act (ERISA)
- Occupational Safety and Health Administration (OSHA)
- Sarbanes-Oxley Act (SOX)
- SSAE-18
- Title VII of the Civil Rights Act of 1964
- US Department of Treasury Regulations
- US Patriot Act of 2001
- Whistleblower Protection Act of 1989

US Financial Laws and Regulations

- Fair Credit Reporting Act (FCRA)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Reserve
 - Electronic Fund Transfers Act (EFTA)
- Federal Trade Commission (FTC)
 - Fair and Accurate Credit Transactions Act (FACTA)
 - Fair Credit Reporting Act (FCR))
 - Fair Debt Collection Practices Act (FDCPA)
- Financial Crimes Enforcement Network (FinCEN)
- NACHA Rules
- State Money Transmitter Licenses
- U.S. Department of Treasury
 - Bank Secrecy Act (BSA)
- US Securities Exchange Commission (SEC)
 - Anti-Corruption
 - Insider Trading
 - Regulation Fair Disclosure (FD)
 - Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank)

Payment Card Brands

- American Express
- Discover
- Japanese Card Brand (JCB)
- Mastercard
 - Merchant Compliance
- Visa
 - Merchant Compliance
- Payment Card Industry Security Standards Council (PCI SSC)
 - PCI Data Security Standards (PCI DSS)
 - Payment Application Data Security Standards (PA-DSS)
 - Point 2 Point Encryption (P2PE)
 - Personal Identification Number (PIN)

Standards

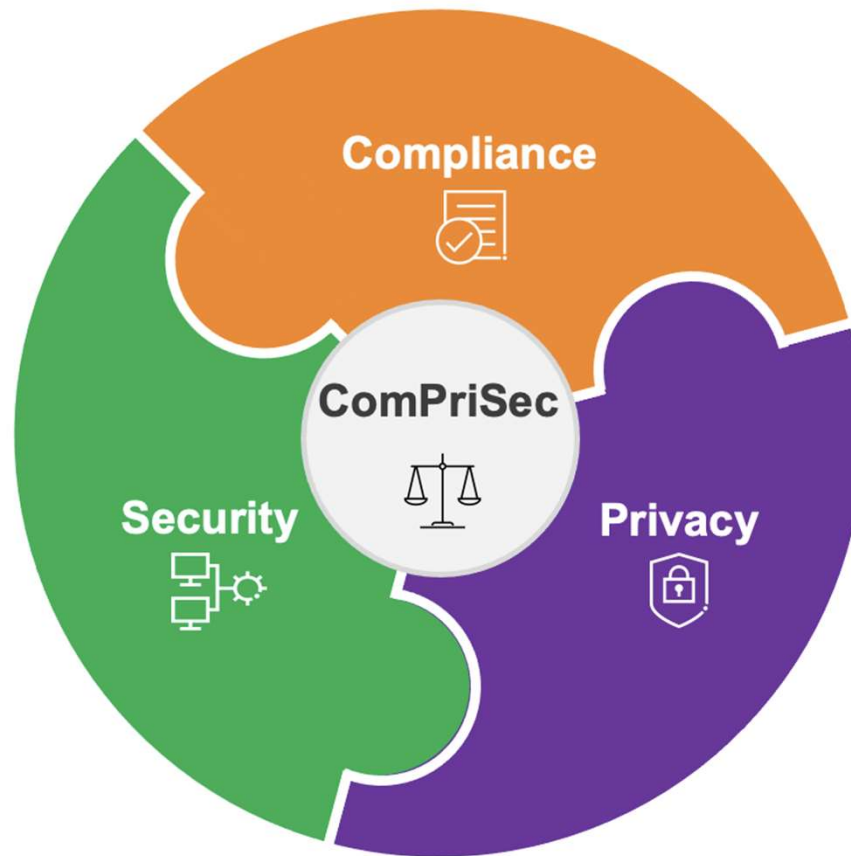
- International Standards Organization 27001 and 27002 (ISO)
- National Institute of Standards and Technology (NIST)
- Open Web Application Security Program (OWASP)
- Accredited Standards Committee X9 (ACS X9)
- American National Standards Institute (ANSI)

Dumpster Fire!



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

ComPriSec[®] = Compliance + Privacy + Security



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

Data

Assets

Harms &
Threats

Controls

Remediation

Third Parties

Laws,
Regulations,
Standards


Requirements

A close-up photograph of a person's hand holding a silver pen, signing a document. The person is wearing a diamond ring on their ring finger. The document is open, and the background is blurred, showing other people in a professional setting.

CONTRACTS

- Roles & Responsibility Matrix
- Service Level Agreements (SLA's)
- Recovery Time Requirements
- Data Storage Locations
- Compliance Requirements
- Vendors
- Right to Audit Clause
- Breach Notification
- Incident Definition & Resolution

Sample Roles & Responsibilities Matrix



Information Supplement • Third-Party Assurance • August 2014

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
System Components (e.g., Firewalls, Servers, Applications, Appliances)				
Determine the procedures for the design, staging, implementation, and ongoing maintenance of system components.	<ul style="list-style-type: none">• Firewall Reviews• Encryption of transmissions over public networks and end user messaging systems• System updates and maintenance including<ul style="list-style-type: none">◦ Patching cycles◦ Operating system vs. application◦ Virtual vs. physical◦ Centralized tools and reporting• Isolation strategies (segmentation, intrusion detection/prevention)• Change management procedures• Anti-virus deployment strategies• Change-detection strategy for critical files• Risk-based analysis including risk-assessment results• Access control procedures• Defining roles<ul style="list-style-type: none">◦ Approval process◦ Entitlement reviews◦ Revocation procedures◦ Two-factor requirement◦ ID and password requirements◦ Session timeouts and login requirements◦ Incident response• Time synchronization (Network Time Protocol)			

https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf



Vetting Third Parties



Due Diligence
Reviews



Compliance



Risk Ratings

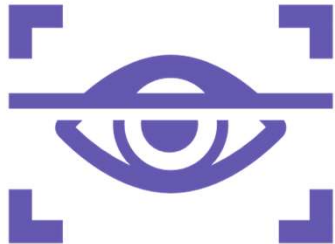


Third Party
Evaluations



ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

Third Party Due Diligence Reviews



Brand



<https://www.cioinsight.com/security/linking-breaches-brand-reputation-stock-prices/>

Financial



<https://www.phillipsfinancialstrategies.com/?redirectUrl=/blog/budgeting-as-financial-planning/>

Location

Caution
October 19, 2023

Update
January 10, 2024

Worldwide Caution
Information for U.S. Citizens in the Middle East

Home | Travel Advisories | Newsroom | About Us | Contact Us | Careers | MyTravelGov | U.S. Department of State | U.S. Embassies & Consulates

Travel.State.Gov
U.S. DEPARTMENT OF STATE — BUREAU OF CONSULAR AFFAIRS

Search

U.S. Passports

International Travel

U.S. Visas

Intercountry Adoption

International Parental Child Abduction

Replace or Certify Documents

Travel.State.Gov > Travel Advisories

Share this page:

Travel Advisories

Travel Advisories

Learn about your destination

Country or area

Filter Travel Advisories

Advisory	Level	Date Updated
Liechtenstein Travel Advisory	Level 1: Exercise Normal Precautions	July 26, 2023
North Macedonia Travel Advisory	Level 1: Exercise Normal Precautions	July 26, 2023
Nauru Travel Advisory	Level 1: Exercise Normal Precautions	July 24, 2023
Palau Travel Advisory	Level 1: Exercise Normal Precautions	July 24, 2023
Burma (Myanmar) Travel Advisory	Level 4: Do Not Travel	January 22, 2024
Worldwide Caution	Caution	October 19, 2023
Afghanistan Travel Advisory	Level 4: Do Not Travel	December 18, 2023
Albania Travel Advisory	Level 2: Exercise Increased Caution	July 26, 2023
Algeria Travel Advisory	Level 2: Exercise Increased Caution	July 13, 2023
Andorra Travel Advisory	Level 1: Exercise Normal Precautions	July 26, 2023
Angola Travel Advisory	Level 2: Exercise Increased Caution	July 24, 2023
Appuila Travel Advisory	Level 1: Exercise Normal Precautions	July 17, 2023
Antarctica Travel Advisory	Level 2: Exercise Increased Caution	January 19, 2023
Antigua and Barbuda Travel Advisory	Level 1: Exercise Normal Precautions	July 17, 2023
Botswana Travel Advisory	Level 1: Exercise Normal Precautions	July 31, 2023
Cabo Verde Travel Advisory	Level 1: Exercise Normal Precautions	July 31, 2023
Comoros Travel Advisory	Level 1: Exercise Normal Precautions	July 31, 2023
Diboni Travel Advisory	Level 1: Exercise Increased Caution	July 31, 2023
Equatorial Guinea Travel Advisory	Level 2: Exercise Increased Caution	July 31, 2023
Guinea Travel Advisory	Level 3: Reconsider Travel	December 26, 2023
Lesotho Travel Advisory	Level 1: Exercise Normal Precautions	July 31, 2023

Take 90 Seconds for Safer Travel

WITH COUNTRY INFO, EMBASSIES, AND CONSULATES

Travel Advisory Levels

1 Exercise normal precautions

2 Exercise increased caution

3 Reconsider travel

4 Do not travel

TRAVEL ADVISORIES AND ALERTS: THE DETAILS

https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

30 | Copyright © 2024 ISACA. All rights reserved.

Security

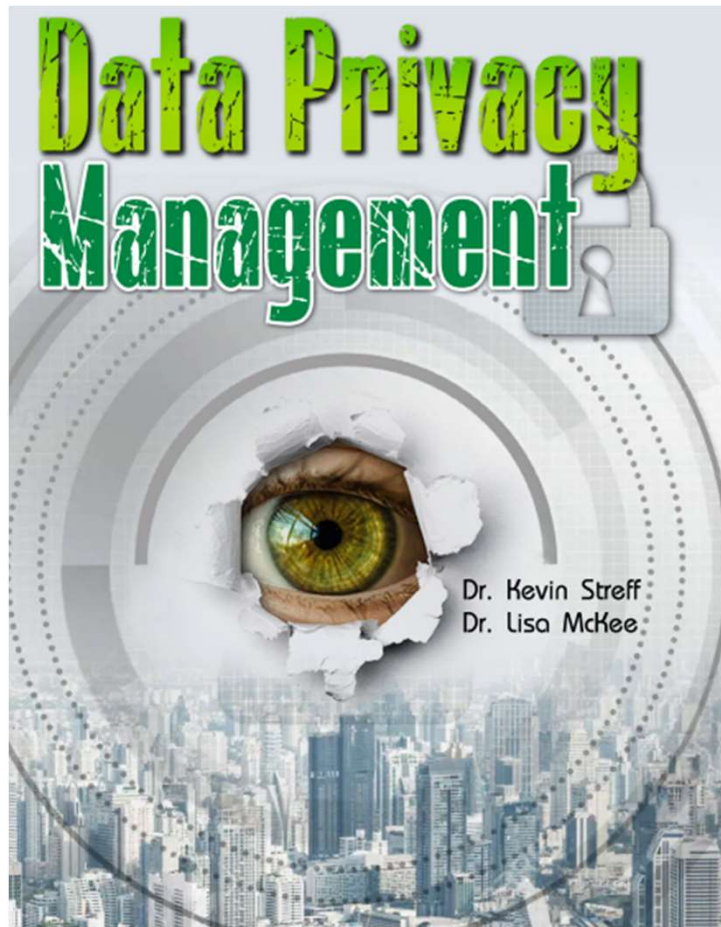


ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



<https://infinitybusinessbrokers.com/why-cybersecurity-is-important-for-small-business-too/>

Privacy



<https://infinitybusinessbrokers.com/why-cybersecurity-is-important-for-small-business-too/>

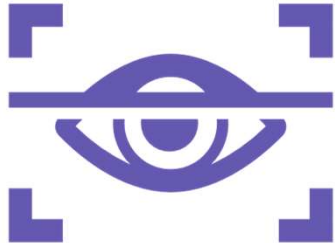


ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

Compliance



Risk Rating

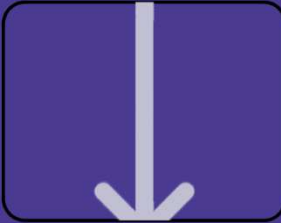


Program Outcomes



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

Executive Support



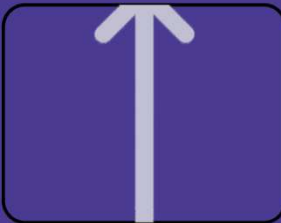
Top Down

- Board Approval
- Executives



Meet in the Middle

- VPs
- Managers



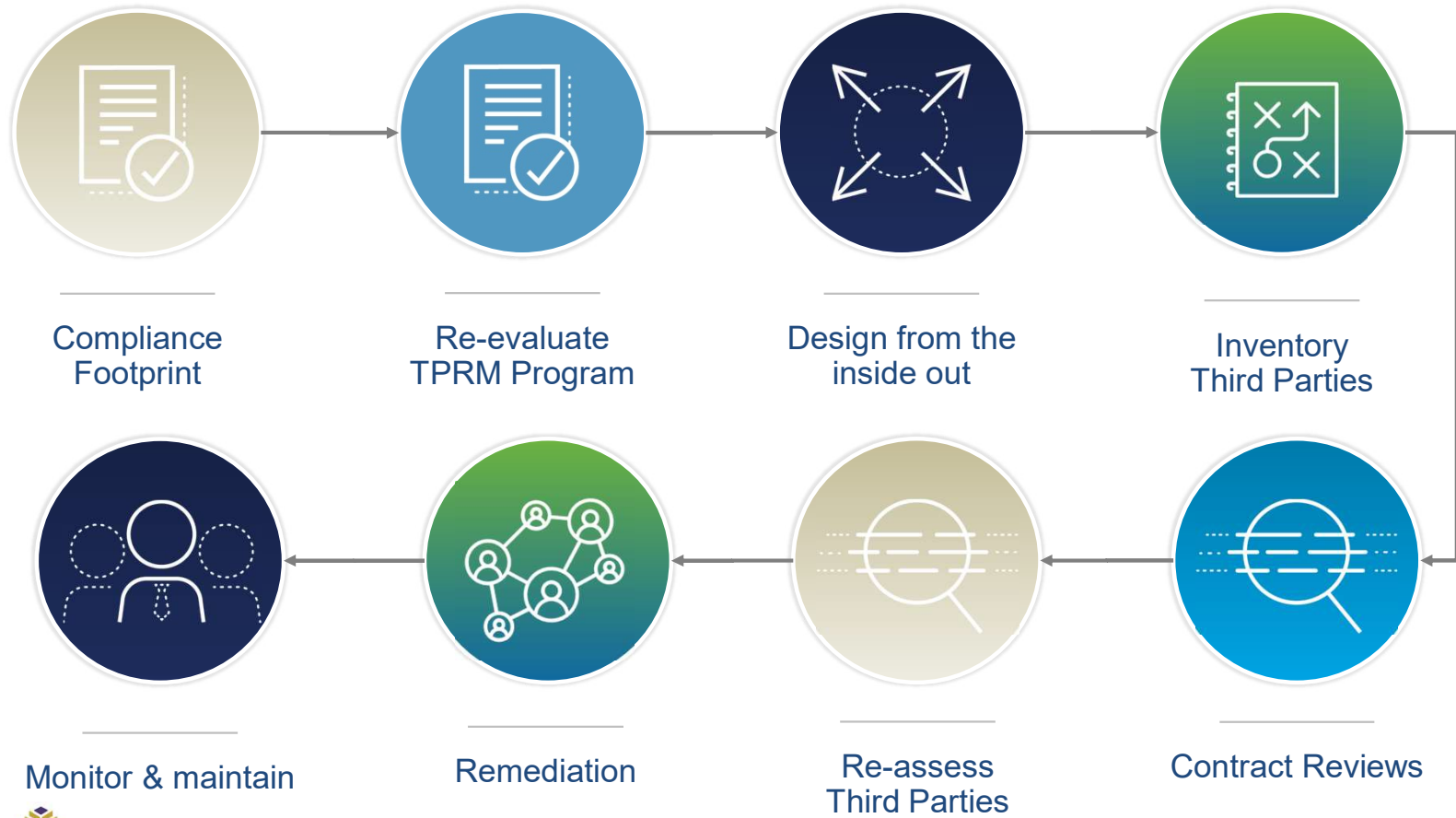
Bottom UP

- Front Lines



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust

TPRM for ComPriSec® Action Plan



Putting it into Practice!

- 3 months – document the organizational obligations, compliance footprint
- 6 month – evaluate and enhance the existing third-party risk management program
- 9 months – review third party contracts to determine where changes are needed
- 12 months – assess third parties based on the updated risk program
- 18 months – monitor third parties and program maintenance



ISACA 2024
NORTH AMERICA
CONFERENCE
In Pursuit of Digital Trust



Connect with Me!

Reach out to the speaker to learn more about their background



Dr. Lisa McKee

American Security and Privacy | Founding Partner
Assistant Professor Cybersecurity | Bellevue University

Lisa.McKee@AmericanSecurityandPrivacy.com

Lisa.McKee@Bellevue.edu

[Research, Publications & Textbook](#)

[Connect on LinkedIn](#)





ISACA 2024
**NORTH AMERICA
CONFERENCE**
In Pursuit of Digital Trust

Thank you for attending!

Dr. Lisa McKee Ph.D., CISA, CDPSE, CRISC