Learn to Assess Third Party Risk (GRC Skills)

Daisy chain of supply chain reliance, the threat of complexity, magnificent 7 concentration risk and more

Steve McMichael
December 28, 2024

Hey there,

Did you catch Dr. Gerald Auger's excellent video on Third Party Risk Management (TPRM)? It's yet ***another*** Simply Cyber *must watch*, not just because of the valuable knowledge you can apply, but it's 100x more fun that anything else YouTube has seen on the topic! Cool also that TryHackMe gave the GRC domain a nod by including this module in *Advent of Cyber*. It's a concrete step towards GRC getting more "socially acceptable" to quote Dr. Auger, or recognized as being *awesome and underrated* as I like to say.

Why does TPRM (also called SCRM - Supply Chain Risk Management) matter? We see supply chain cybersecurity incidents in headlines everyday, and we're only getting ***more*** dependant on third parties. 📈

One driver is complexity, which NIST Fellow Dr. Ron Ross points out is the biggest cyber threat we face today:

> Trillions of lines of code in billions of devices, with ubiquitous connectivity across the globe.
>
> Dr. Ron Ross

Another is concentration risk associated with the "*magnificent 7*" tech titans that have emerged in our economy, that are uniquely positioned for further industry disruption with AI, beyond what what we've already experienced with cloud, mobile and other big transformations.

> The Magnificent Seven contributed 58% fo the S&P 500's total return in 2023. Historically, the top 10 stocks in the S&P500 contribute 14% of the index's total return, showing the current over-concentration
>
> Dan Irvine, Principal, 3Summit Investment Management investopedia.com

Investopedia TRADE

TABLE OF CONTENTS

Historical Performance of the Magnificent 7 Stocks

The table below displays the performance of the Magnificent Seven stocks over the last six months, one year, and five years.

Magnificent Seven Stock Performance (6 months, 1 year, 5 years)

Name	6 Months (%)	1 Year (%)	5 Years (%)
Alphabet Inc. (GOOG)	31.77%	57.31%	241.22%
Amazon Inc. (AMZN)	26.46%	50.52%	104.61%
Apple Inc. (AAPL)	9.98%	14.72%	331.31%
Meta Platforms Inc. (META)	42.93%	81.95%	170.72%
Microsoft Corp. (MSFT)	20.26%	36.25%	236.55%
NVIDIA Corp. (NVDA)	153.75%	209.81%	3,130%
Tesla Inc. (TSLA)	-23.02%	-19.27%	1,240%

Data as of June 26, 2024 (source: TradingView)

https://www.investopedia.com/magnificent-seven-stocks-8402262#toc-historical-performance-of-the-magnificent-7-stocks

The growing importance of SCRM for these reasons and more is why we saw NIST Cybersecurity Framework increase emphasis on it both in their version 1.1 in 2018 and 2.0 in 2024.

In this blog I'll provide my perspective on key points Dr. Auger walks through, and connect it to *Mastering Cyber Resilience* material and my experiences, to drive these concepts home to help you maximize outcomes as a GRC practitioner or a cybersecurity consultant.

Check it out and let me know what you think!

Be safe, be well,

Steve

Contents

- What is GRC?
- Mission Impossible? Unlimited Cyber Threats vs Lim …
- Governance Explainer
- Compliance Explainer
- Risk Explainer
  - Risk Assessments
- Spreadsheets (Like GRC) Are Awesome and Underrated …
  - 1. XLOOKUP
  - 2. Pivot Tables
- Vendor Security Questionnaire Assessment
  - Question 1: PR.DS Protecting Data in Transit and a …
    - NIST CSF Category Lookup: PR.DS-01 and PR.DS-02
      - Informative References
        - CIS Controls
          - Encryption in transit examples:
          - TLS (Transport Layer Security)
          - SSH (Secure Shell)
          - Encryption at rest examples:
        - NIST SP 800-53
          - SC-12 Cryptographic Key Establishment and Manageme …
          - Asymmetric Encryption
          - Symmetric Encryption
          - SP 800-56A: Recommendation for Pair-Wise Key Estab …
          - FIPS-197: Advanced Encryption Standard (AES)
          - FIPS-198: The Keyed-Hash Message Authentication Co …
          - SP 800-56B: Recommendation for Pair-Wise Key Estab …
          - NIST SP 800-56C: Recommendation for Key-Derivation …
  - Question 2: PR.AA-05 Access Permissions | Principl …
    - NIST CSF Category Lookup: PR.AA-05

- Informative References
    - CIS Controls v8.0:
    - SP 800-53 Rev 5.1.1:
- Question 3: ID.AM-8 Data Lifecycle | Securely Disp …
    - NIST CSF Category Lookup: ID.AM-08
        - Informative References
            - CIS Controls v8.0: 1.1 CIS Controls v8.0: 3.5
            - SP 800-53 Rev 5.1.1:
- Conclusion: Crushed it! 🥊

What is GRC?

> GRC is an acronym that stands for Governance, Risk, and Compliance. Each of these are kind of independent of each other and we'll break down each of them. But they basically ensure that an organization has a methodical and intelligent approach to driving cyber risk reduction.
>
> Dr. Gerald Auger

Mission Impossible? Unlimited Cyber Threats vs Limited Resources

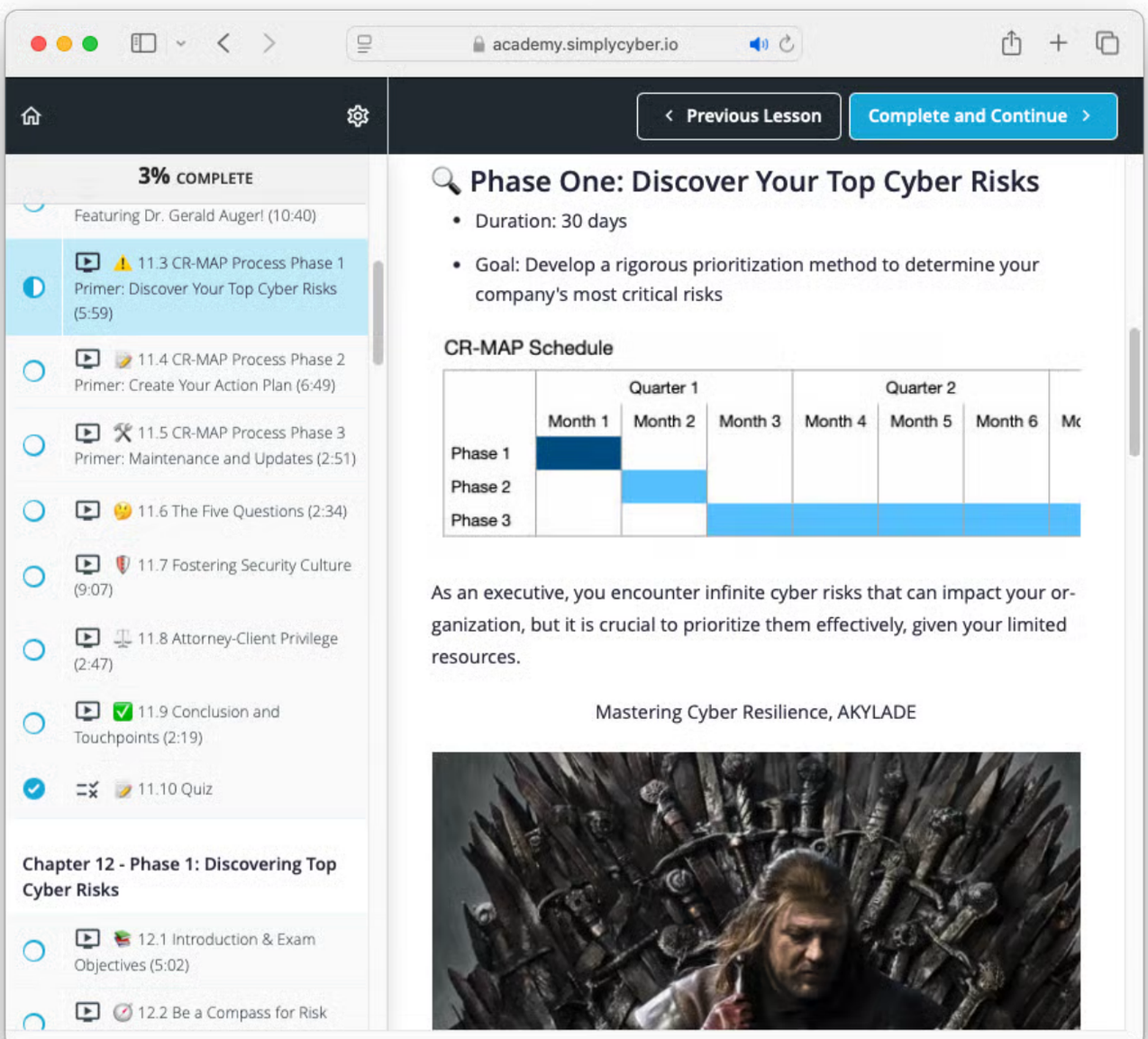
As the cliche goes, cybersecurity is hard.

Why Cybersecurity is Hard

www.cpatocybersecurity.com/p/why-cybersecurity-is-hard

Two key points to wrap our heads around in the context of this lesson:

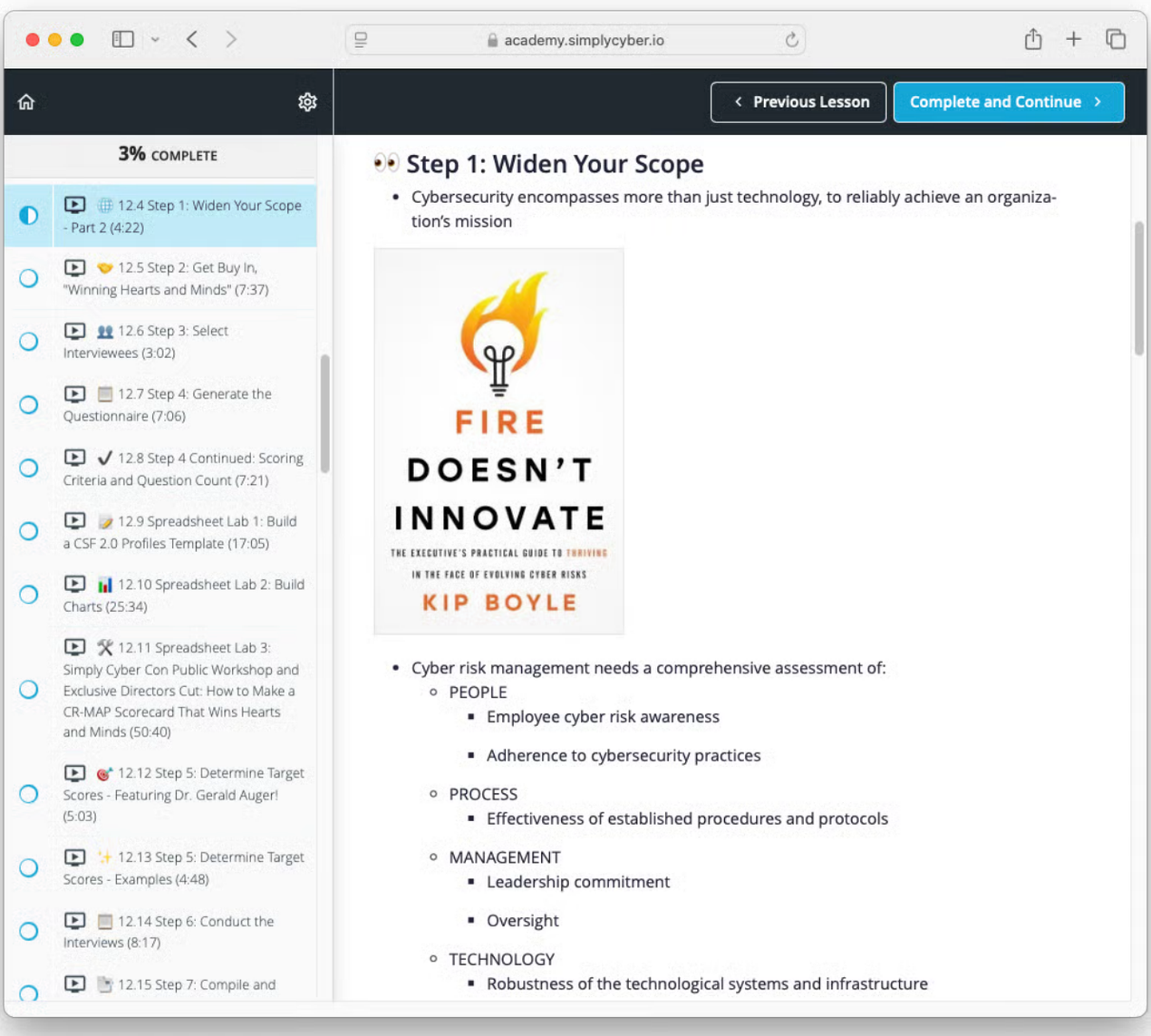
1. It's not JUST that there's infinite cyber risk and limited resources



2. Cybersecurity and cyber resilience are not something that you can just write a cheque to solve faster

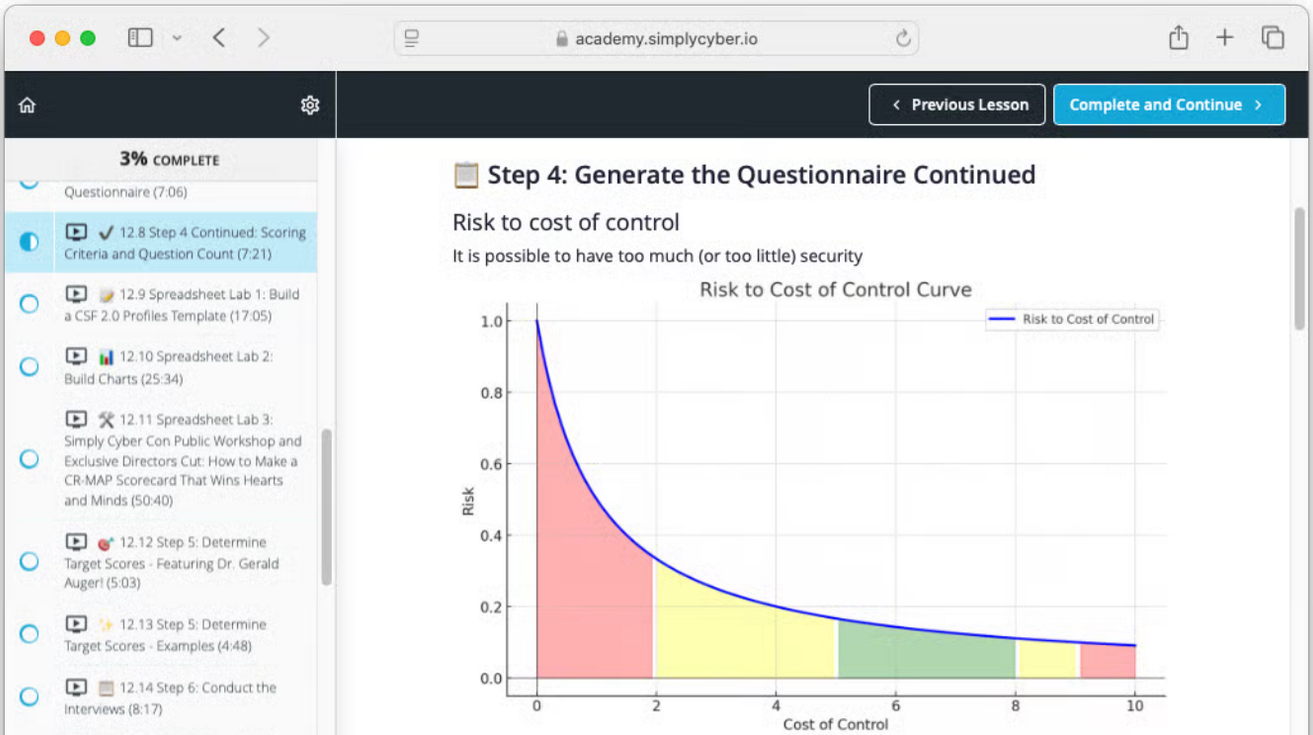
> Even if you had infinite money - here's a blank check, go buck wild, you got a genie with three wishes and the first wish you wish for is infinite money, good for you - you know what you can't do?
>
> You can't buy all the tools. You can't train all the staff. You can't keep staff who know what they're doing there because they might go to another place. So infinite money doesn't equal infinite security.
>
> Dr. Gerald Auger

- It's like the project management analogy that pregnancy takes 9 months - you can't spend money to shorten that timeframe
- Or the saying that "you can't rack and stack security culture" - it's not something you can buy off the shelf and plug in.
- As Kip Boyle points out in *Fire Doesn't Innovate* and *Mastering Cyber Resilience*, cyber risk management needs a comprehensive assessment of people, process, management and technology



> But in reality, we don't have infinite money. We don't have infinite resources or infinite time. So what we need to do is figure out where we need to spend our money, what we need to prioritize first, and who's going to do the work and how they're going to do it. This is what GRC basically is - looking at and thinking of.
>
> Also, bonus tip: there's actually academic research that shows there's diminishing returns the more money you put in. I.E. if I give you a million dollars, you can get your InfoSec program to pretty good. If I gave you another million dollars, you wouldn't double the effectiveness of your cyber program. It would only be like a percentage of that. So there's a logarithmic curve.
>
> Dr. Gerald Auger, PhD

- Identifying reasonable places in the risk to cost of control curve, in the trade-off of protecting and enabling the business is the key
- The 0-10 score key in *Mastering Cyber Resilience* from Insecurity to Too Much Security is a helpful guide to find the appropriate Goldilocks zone in your assessments
- This score key is included in my Simply CYBERCON workshop, *How to Make a Cyber Risk Scorecard that Wins Hearts and Minds*



12.15 Step 7: Compile and Average the Scores (2:23)

12.16 Step 8: Communicate Your Top 5 Cyber Risks (6:17)

12.17 Part 1: EXCLUSIVE TO SIMPLY CYBER ACADEMY: Analyzing Network Diagrams - Featuring Dr. Gerald Auger! (8:08)

12.17 Part 2: EXCLUSIVE TO SIMPLY CYBER ACADEMY: Analyzing Network Diagrams - Featuring Dr. Gerald Auger! (17:49)

12.18 Conclusion and Touchpoints (1:53)

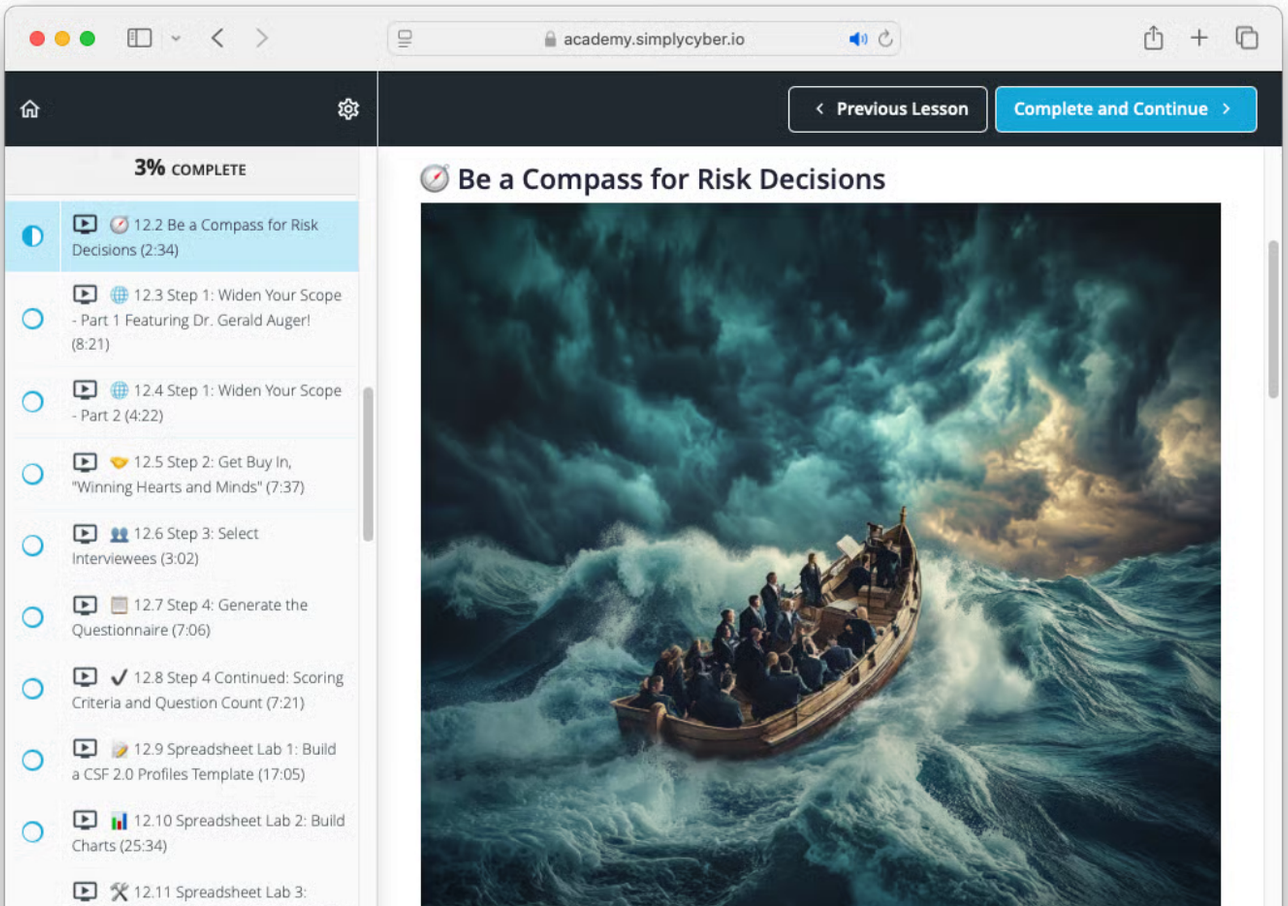
Score	Description	How Secure (Resilient)?
0-1.9	Insecurity	Not Enough
2.0-4.9	Some Security	
5.0-5.9	Minmially Acceptable Security	Just Right
6.1-6.9	Optimized Security	
7.0-7.9	Fully Optimized Security	
8.1-9.0	Too Much Security (Waste)	Too Much
9.1-10.0		

The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win

Governance Explainer

Governance is basically what are the rules of the business and what is the attitude of the business? What is normal at this business? And then having leadership be like, "No, this is important."

- You've heard that cyber risk management is the *perfect storm*
- Your Cyber Risk Management Action Plan work provides the executive team a compass to steer through it

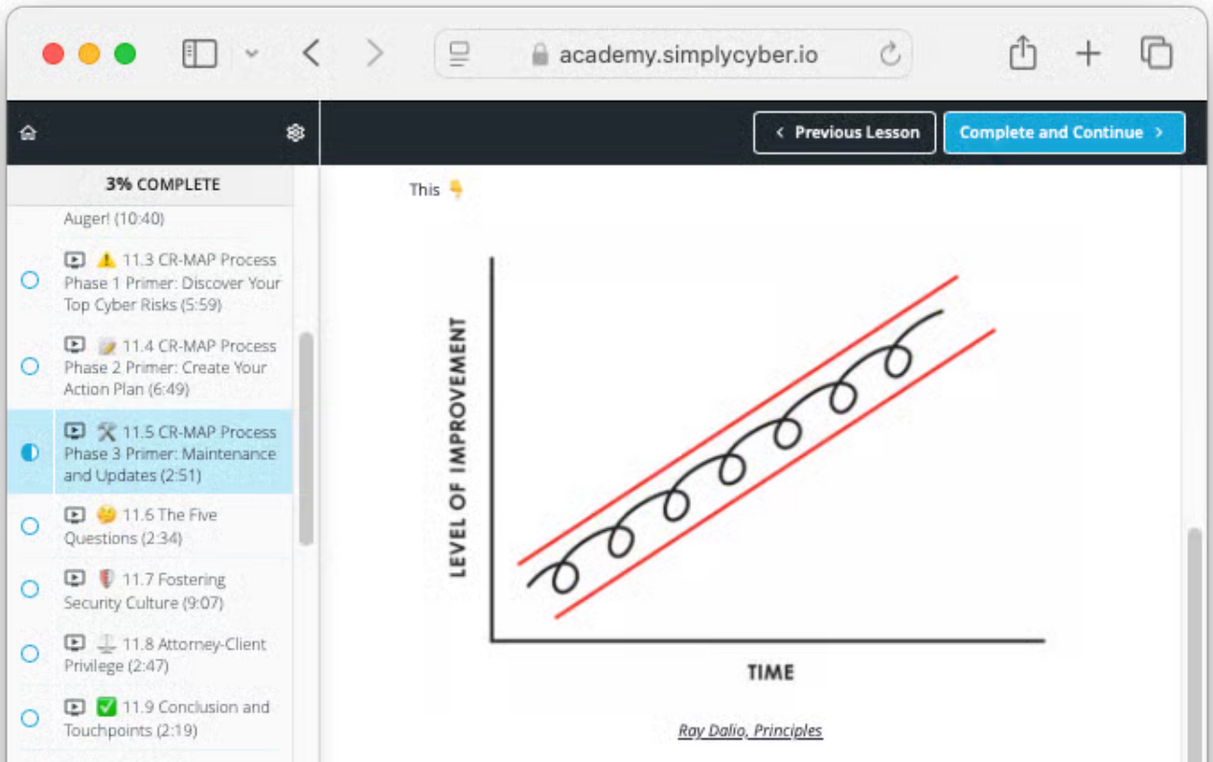


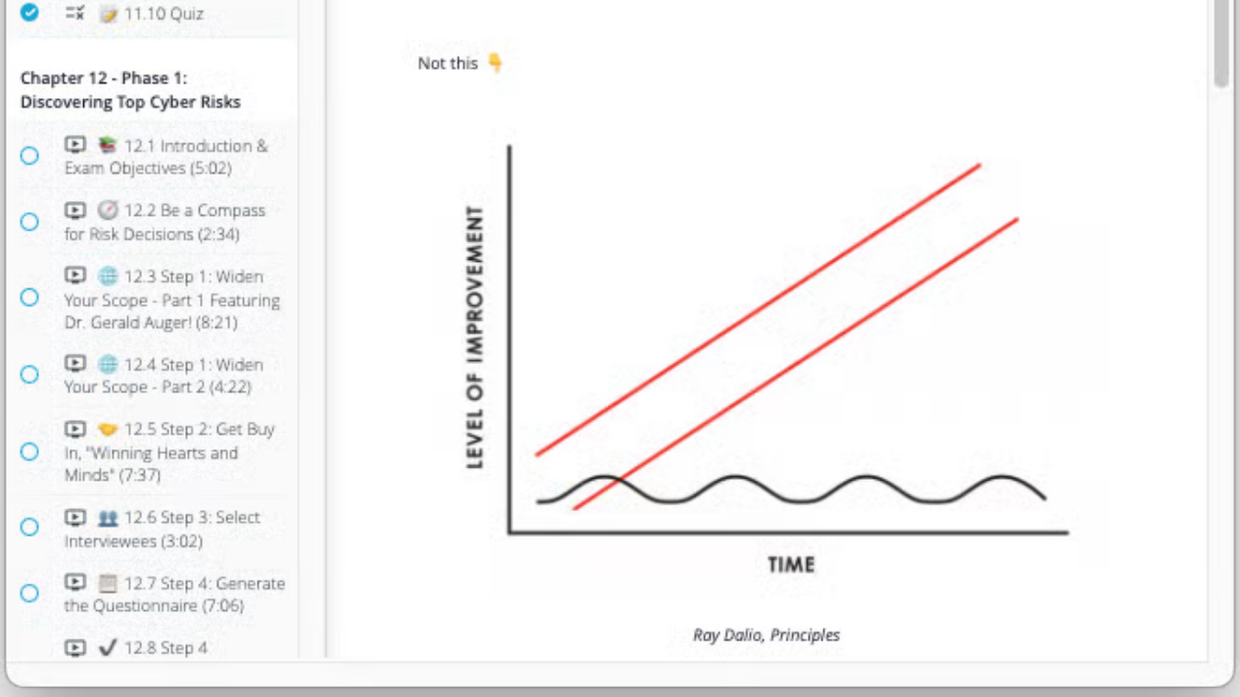
Governance can also include frameworks. I'm a huge fan of the NIST Cybersecurity Framework and CIS Top 18.

Frameworks are great and it allows you a repeatable, mature process in order to grow into a mature InfoSec program and make sure that you're hitting comprehensively all the elements of a cyber program. Making sure that you're looking at people, process, technology - not just saying "Oh, we're taking backups and we've got multi-factor, we're good to go." Yeah, okay, but are you doing configuration management? Are you doing vulnerability management? Are you regularly pen testing your environment? Are you doing risk assessments? Who's allowed to access what? Do you revoke credentials if they get compromised? Who's allowed to do that? A million things!

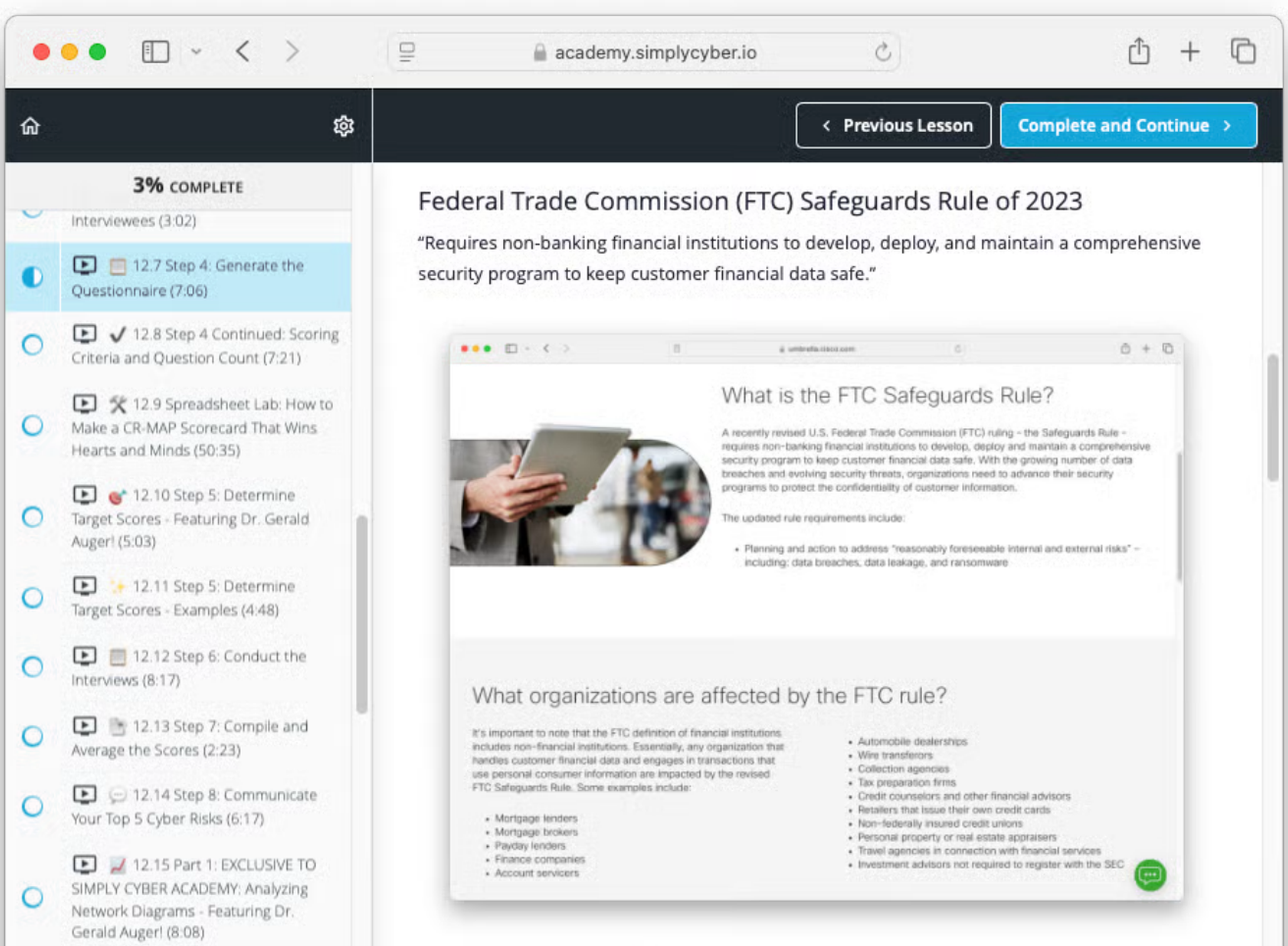
Dr. Gerald Auger

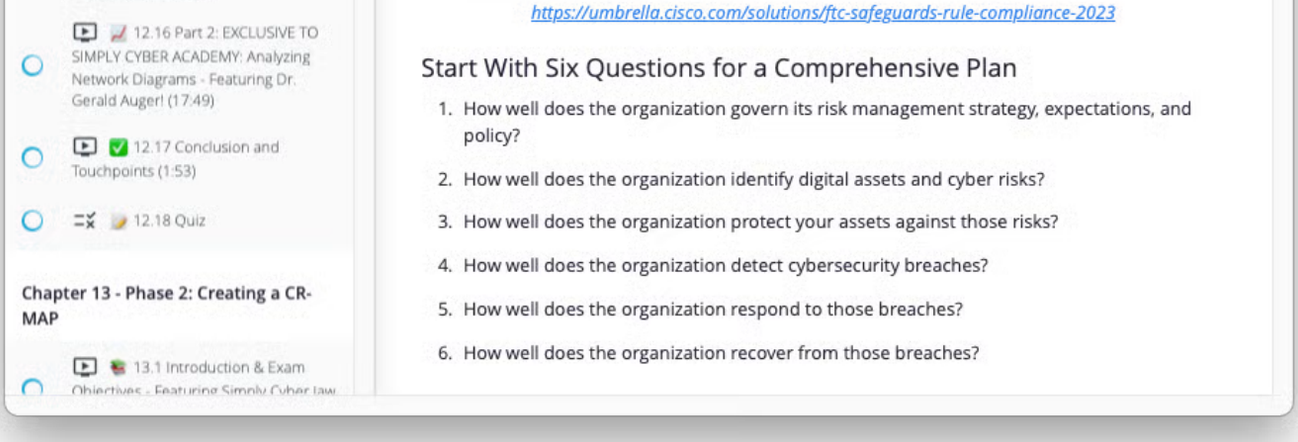
- Follow the Simply Cyber mantra “Lather, rinse, repeat” to grow into a mature InfoSec program!





- Being comprehensive is key for demonstrable due diligence and due care
- That "comprehensive" word pops up in places like the *FTC Safeguards Rule* of 2023 for financial data, that is used in the court of law and the court of public opinion



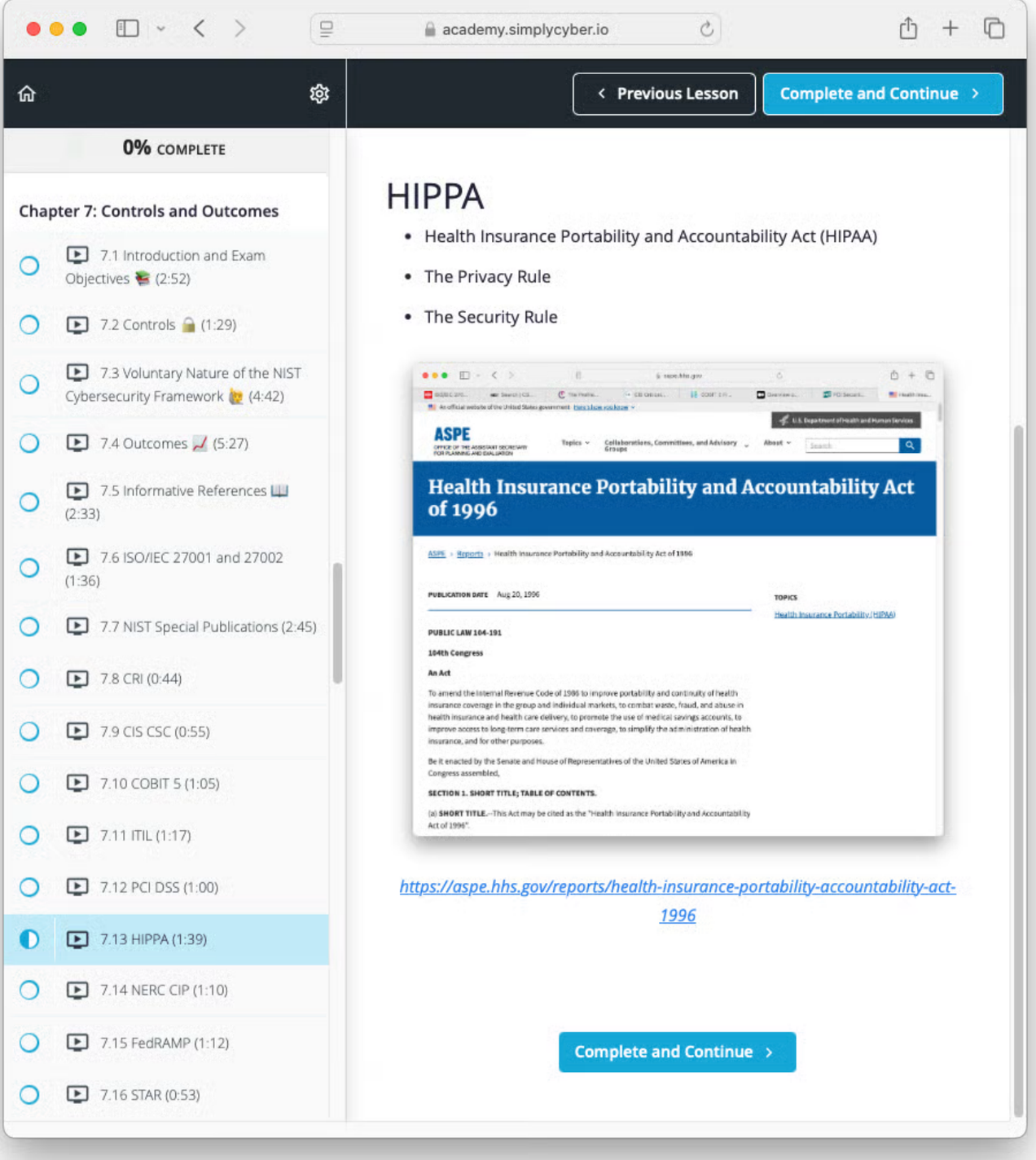


- Another insight related to comprehensiveness in the Governance function, is establishing clear expectations in policies
- Turn on your negative mindset for a moment to risk assess a malicious insider attack scenario, where an insider harms your company and your colleagues, in a way that seems really bad
- If your policies weren't comprehensive enough by being baselined against an industry framework, the justice system is going to have a hard time being effective, because the malicious insider can say, "I didn't know that wasn't' allowed"
- Not legal advice here, of course, but food for thought

Compliance Explainer

> And then finally, compliance. This is like your on-ramp to GRC. Compliance is straightforward. There's a list of documented requirements, whether it's PCI (Payment Card Industry), or it is HIPAA (the Health Insurance Portability and Accountability Act). I don't want to say compliance is easy, but compliance is easy to understand. Here's a bunch of things: are you doing them? Yes or no. This is where a lot of GRC people actually start in their career because you audit against the compliance standard.
>
> Dr. Gerald Auger

Some industry resources to check out here are *ISO27k*, *NIST Special Publications, CRI*, *CIS CSC*, *COBIT 5*, *ITIL*, *PCI DSS*, *HIPPA*, *NERC CIP*, *FedRAMP*, *STAR* and *OWASP*



Risk Explainer

Let's talk about the next one: risk. What is risk? Again, like I said before, you can't secure all the things. You will always, always, always have residual risk. I don't care what you're doing, what industry, what size org - you will always have residual risk. So it's managing how much of that residual risk exists with respect to funding or budget, manpower or person power, and just resources like time and stuff.

"Oh cool, Security Onion, what a great tool! Let's roll it out." Okay, well what are you going to put down in order to roll out Security Onion? "Oh, I didn't think about that." And once you roll it out, who's going to manage it, maintain it, care and feed it? I can't tell you - honestly, quick side note - I can't tell you how many abandoned projects I've seen in my career. People get all geeked up like "Oh, let's roll out Security Onion!" And then like a month later, you've got it rolled out and then nobody's using it because nobody's managing it. And then it's like, "Oh, that was a lot of fun."

Dr. Gerald Auger

- An action plan to implement Security Onion didn't consider people or process elements to go with the technology
  - ➡️ Back to **STEP 1: 👀 Widen Your Scope**
- It also wasn't reasonable and repeatable 🔄, in the appropriate place for the risk to cost of control curve

That's what risk is. We need to understand what is the risk of doing something, what is the risk of not doing something.

Multi-factor authentication - perfect example. In my opinion, should be rolled out everywhere. But maybe some organizations don't want to put it on the executives for whatever reason. They're special snowflakes and they don't want to use multi-factor because it's hard. Well, you could say, "Okay, we are taking on additional risk because

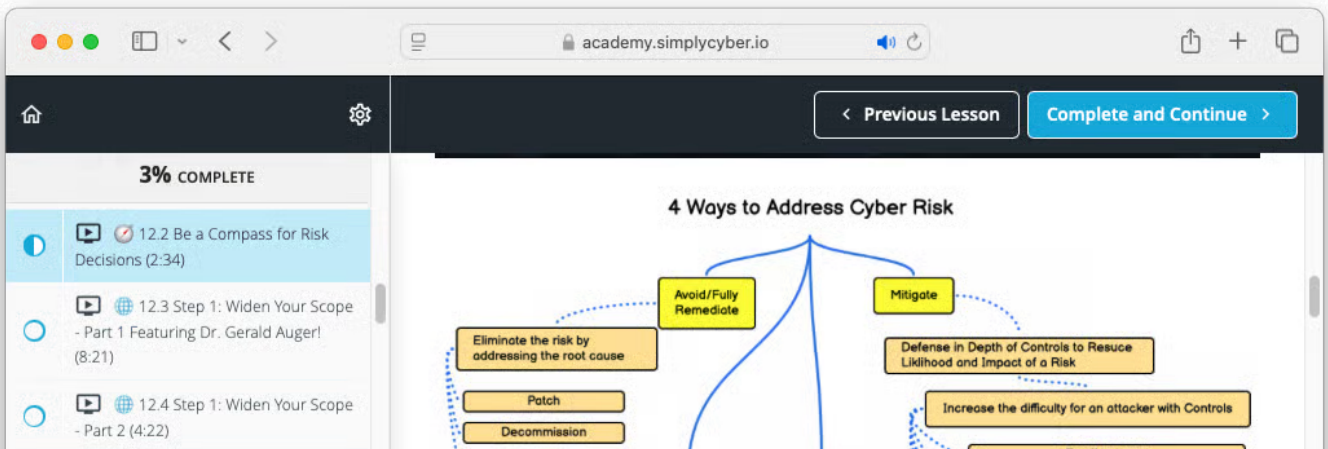
(a) if you reuse passwords or you have crappy passwords, business executives, you're probably going to get your account cracked.

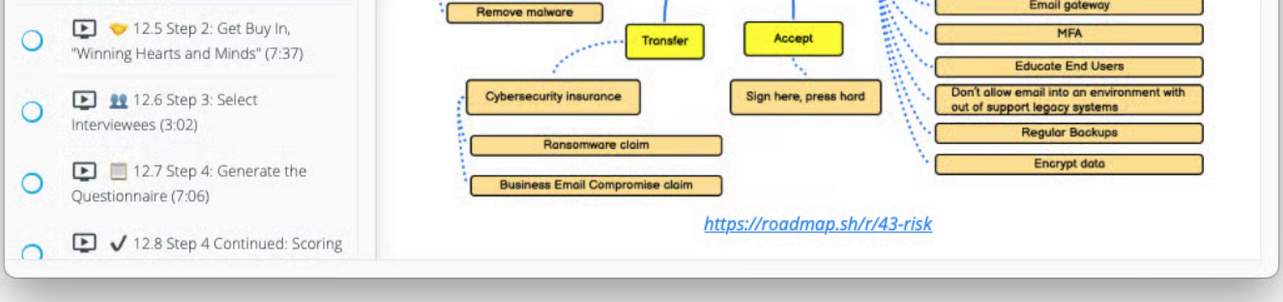
(b) Secondly, without MFA, they're going to walk right through. This could lead to business email compromise, loss of revenue. This could lead to phishing or social engineering of staff and other problems. This could lead to a compromise of reputational harm because you're a publicly traded company and sensitive financial forecasting data gets out because they're in your account."

Is that the kind of risk you want to take on? Maybe you don't say it in that way to the executives - there's a much more polished way to do it. But my point is, this is risk and it's what we GRC folks are responsible for managing, maintaining, and keeping an eye on. Because risk is a very fluid, very dynamic element.

Dr. Gerald Auger

- There are four ways to address cyber risk: mitigate, avoid, transfer or accept
- The default position is acceptance: if your organization isn't cyber threat aware, they might be accepting and holding onto a bigger bag of risk than they realize





- On Dr. Auger's note about having a "polished" way to explain risk treatment options, this is crucial and I don't think well understood
  - Rather than shaming end users and applauding threat actors, dial up your emotional intelligence quotient to meet your audience where they are on cyber risk awareness, and tell them what they need to know
  - Here's my attempt with Uncle Carl at a barbecue

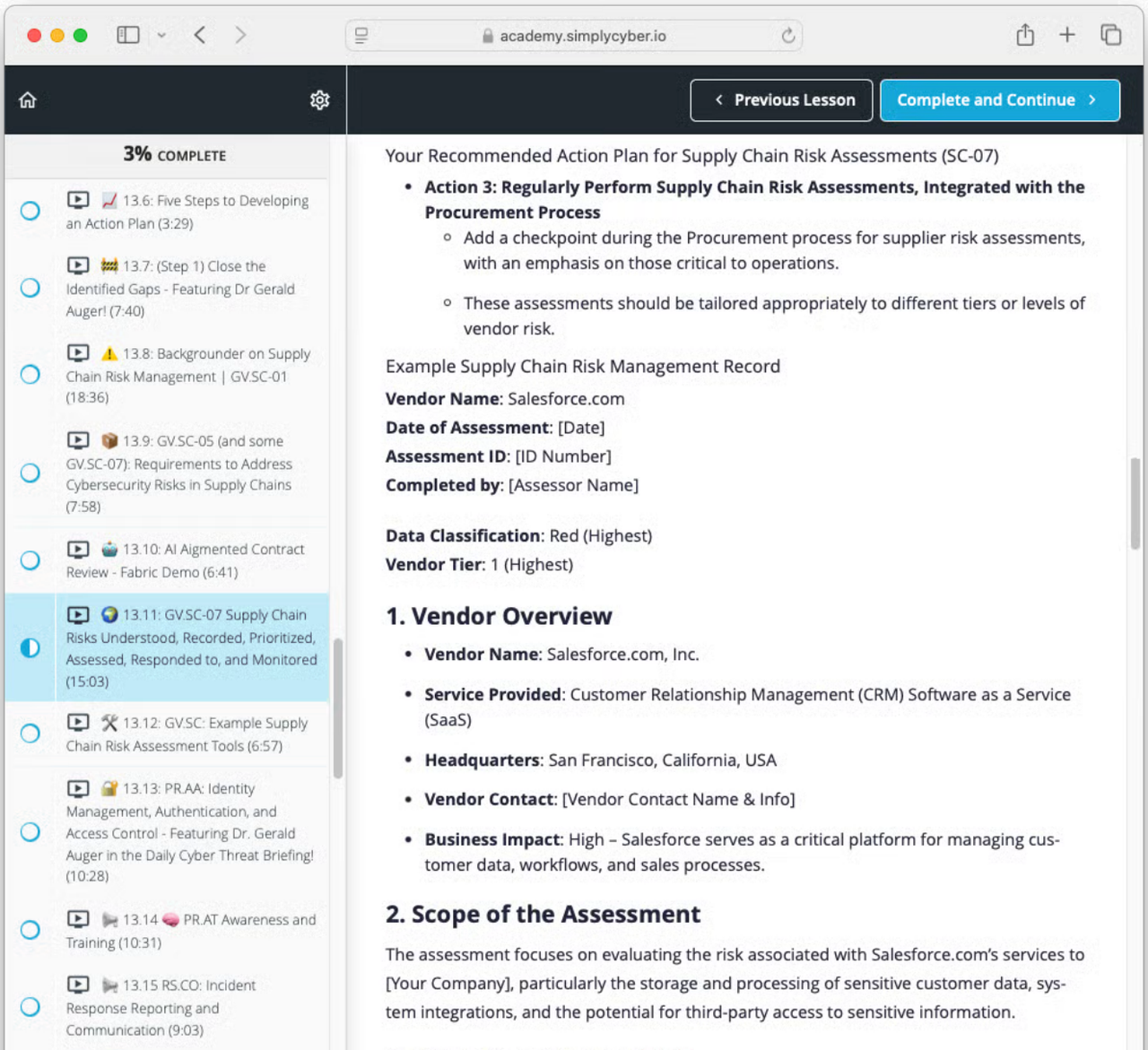
Risk Assessments

Holler! Let's talk risk assessments. Risk assessments is what it sounds like. There's risk - I just flipped out about that for a minute - and a risk assessment is basically a deliberate method of going through and looking at your, you know, either looking at an application, looking at a system, looking at an overall enterprise, and figuring out where the weaknesses are. And then discovering how bad those weaknesses are, specifically, because some weaknesses aren't such a big deal.

Classic example: you got a Windows XP machine running, which would be disgusting, but it's in a lab environment, air-gapped from the internet. Who cares?

> You can see here McSkidy and Grinch are going to basically hand out a third-party questionnaire, which basically gets information solicited from third parties. That information comes in and then based on that information, we're going to assess the risk of their security posture and them holding our data.
>
> Dr. Gerald Auger

- We're getting into **GV.SC-07** here: "The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship"
- Third Party Risk Assessments work well as a checkpoint during the Procurement process, and should be tailored (in terms of due diligence and friction to the business trying to buy something) to the risk level of the third party. RIsk level is commensurate to:
  - The security classification of the data on your network that will traverse to the third parties network
  - Access the third party might require to your network.



Spreadsheets (Like GRC) Are Awesome and Underrated, for Fit-For-Purpose Data Analysis

> Ah, here we go. Be still my heart - the spreadsheet. This is, you know, like if a cowboy has a pistol and a holster on his hip, a GRC professional has a spreadsheet in the holster on the hip. I know there's all sorts of fancy tools, but I'm telling you right now, the spreadsheet - and once you pick up pivot tables, oh my goodness, slow down!
>
> Dr. Gerald Auger

It's so great to find Dr. Auger sharing not just contrarian view point that GRC can make an outsided impact, but Excel too for fit-for-purpose tasks!

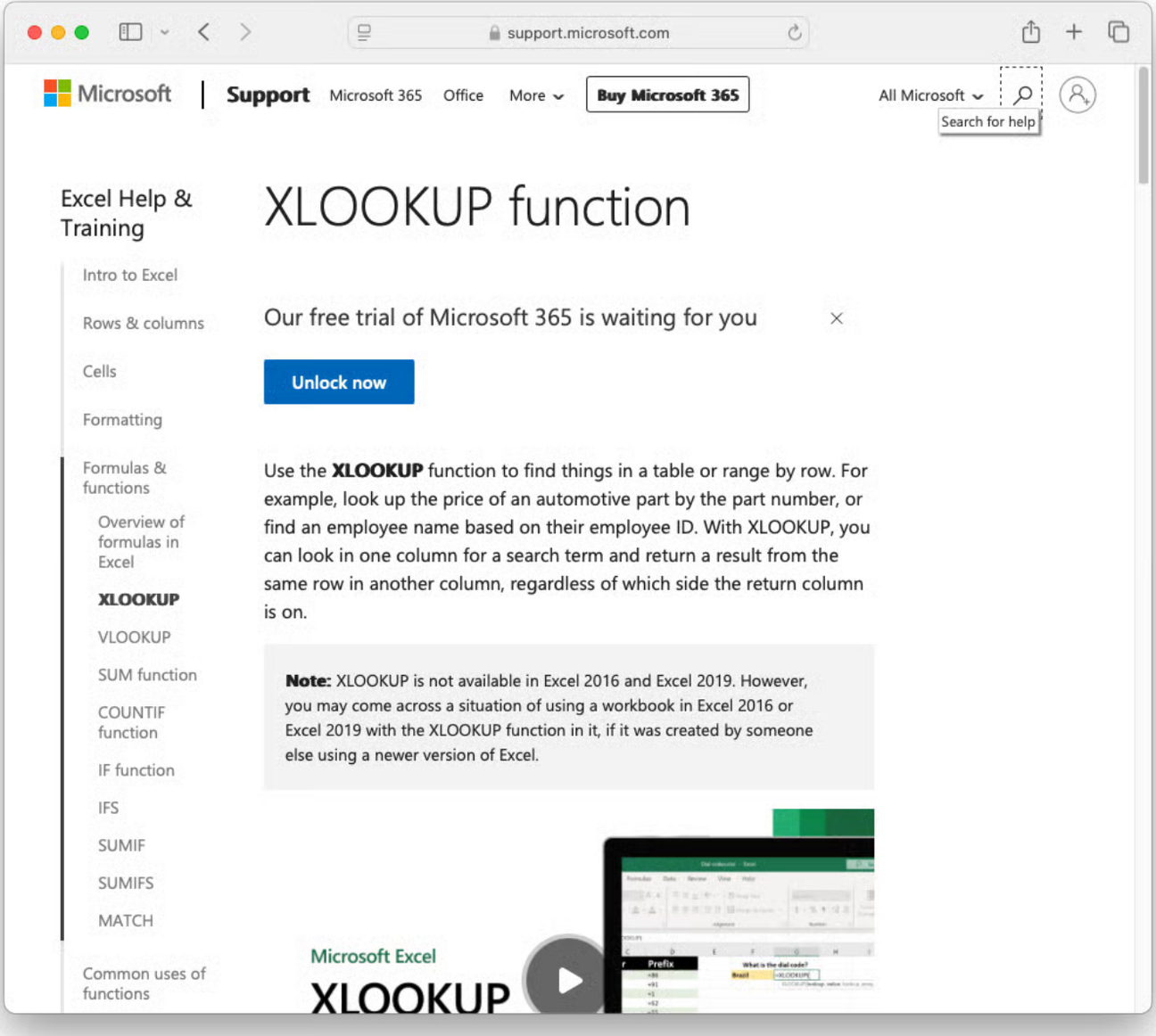
With GRC it's about interfacing between the business and technical teams to prioritize limited resources against unlimited cyber threats. With spreadsheets its about ad hoc data analysis to extract actionable insights from large and disparate data sets. There's a reason Excel is one of the most searched for topics in e-learning.

Just make sure it's the right tool for the job.

To learn about Excel Tables, Slicers, Formulas like XLOOKUP, Pivot Tables, Charts and Power Query so you can "invert the power dynamic between yourself and executives," check out my Simply *CYBERCON workshop* that demonstrates these capabilities, and don't hesitate to let me know if you have any questions.

Or if you just want to know the top 2 highest Return On Investment Data Analytics techniques in Excel, here they are:

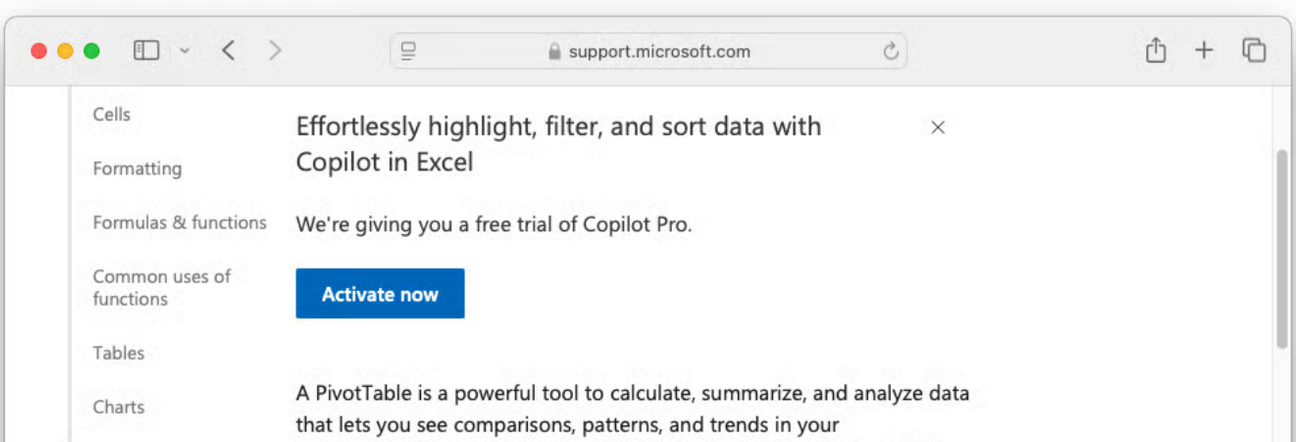
1. XLOOKUP

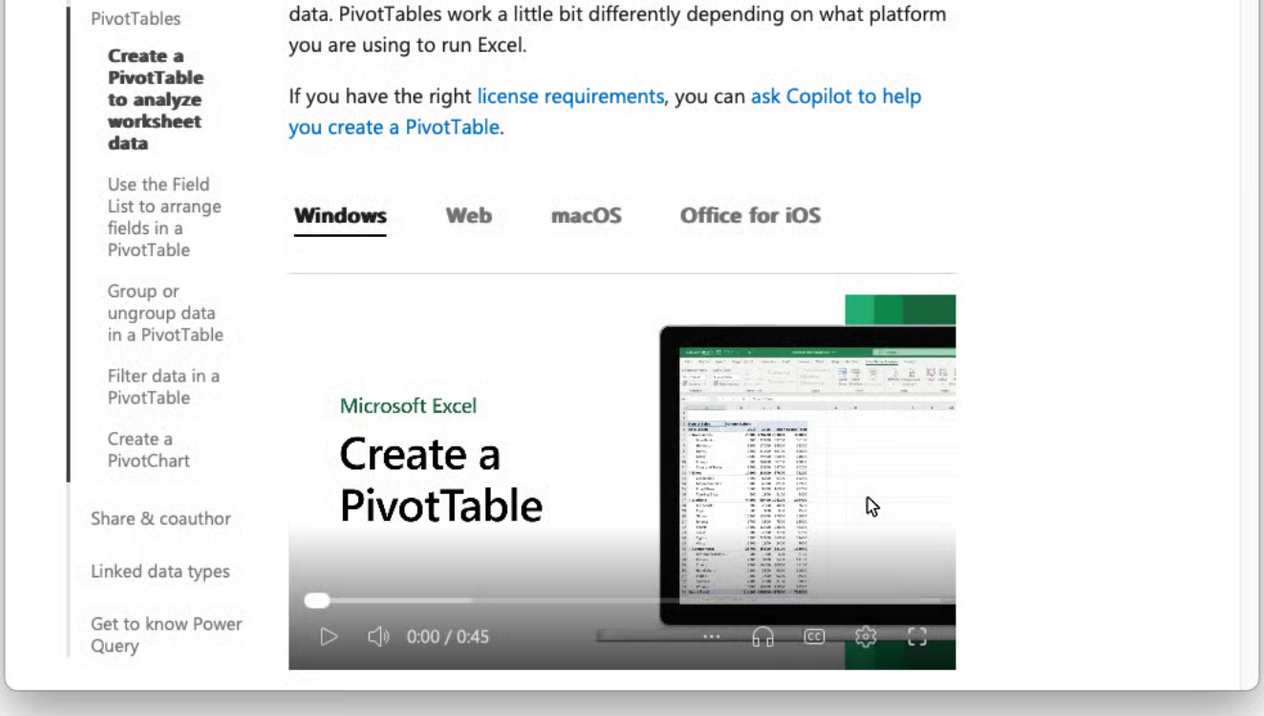


https://support.microsoft.com/en-us/office/xlookup-function-b7fd680e-6d10-43e6-84f9-88eae8bf5929

XLOOKUP is an easier and more powerful, adaptable approach for joining data sets than VLOOKUP, if you've heard of that very popular formula.

2. Pivot Tables





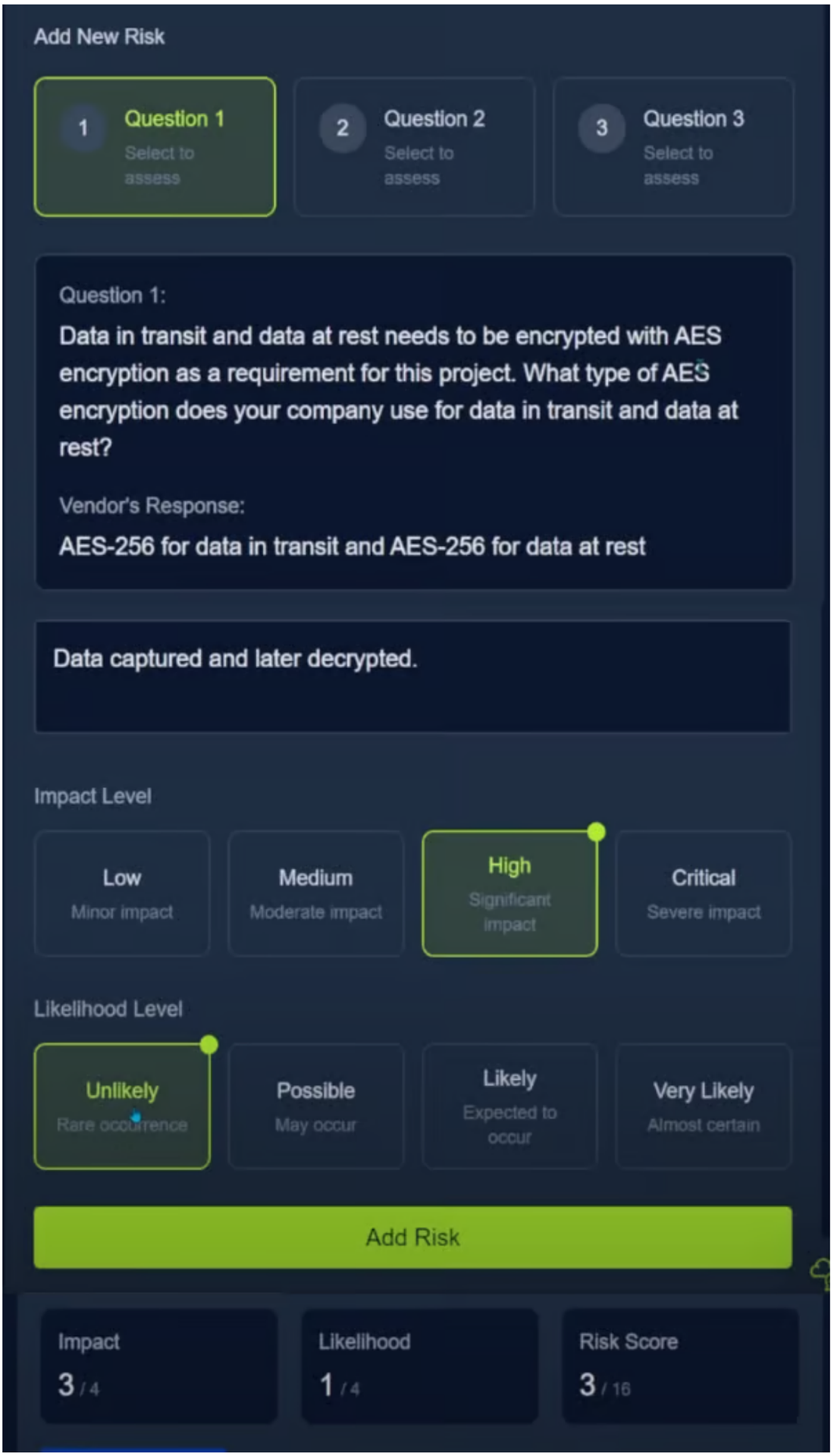
https://support.microsoft.com/en-us/office/create-a-pivottable-to-analyze-worksheet-data-a9a84538-bfe9-40a9-a8e9-f99134456576

Once you have clean and comprehensive underlying data, Pivot tables can quickly extract insights from it, by rolling up, drilling down, slicing and dicing for analysis.

Vendor Security Questionnaire Assessment

Question 1: PR.DS Protecting Data in Transit and at Rest

> We want to know about data in transit and at rest needs to be encrypted with AES as a requirement. Maybe it's contractually required; maybe it's a business policy that you need AES, which is currently considered secure—AES 256 or higher. What type of AES encryption does your company use for data? Remember, they're holding our sensitive data. The vendor response here is AES 256 for in transit and AES 256 for data at rest. This is right on; I like this one.
>
> If the impact were to get compromised, there would be for sure significant impact of the data. The potential security risk here—we're going to document that this is where the GRC risk assessment piece comes in. It's not very high honestly but data captured and later decrypted—I don't think this is very likely to happen honestly. Quantum computers are where we're at right now, so I'll leave this unlikely but the impact would be high if it were to happen. Let's go ahead and click add risk.
>
> Dr. Gerald Auger



NIST CSF Category Lookup: PR.DS-01 and PR.DS-02

csrc.nist.gov

Function

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Category

Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

Category

Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

Category

Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

Subcategory

PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected

Implementation Examples

Ex1: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources

Ex2: Use full disk encryption to protect data stored on user endpoints

Ex3: Confirm the integrity of software by validating signatures

Ex4: Restrict the use of removable media to prevent data exfiltration

Ex5: Physically secure removable media containing unencrypted sensitive information, such as within locked offices or file cabinets

https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

CSF Subcategory ID	Implantation Example(s)
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Ex1: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Ex1: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications

Informative References

CIS Controls v8.0

- 3.11 Encrypt Sensitive Data at Rest

CIS Controls v8.0

- 3.10 Encrypt Sensitive Data in Transit

SP 800-53 Rev 5.1.1

- CA-03: Information Exchange
- CP-09: System Backup
- MP-08: Media Downgrading
- SC-04: Information in Shared System Resources
- SC-07: Boundary Protection
- SC-12: Cryptographic Key Establishment and Management
- SC-13: Cryptographic Protection
- SC-28: Protection of Information at Rest
- SC-32: System Partitioning
- SC-39: Process Isolation
- SC-43: Usage Restrictions
- SI-03: Malicious Code Protection
- SI-04: System Monitoring
- SI-07: Software, Firmware, and Information Integrity

SP 800-53 Rev 5.1.1

- AU-16: Cross-Organization Audit Logging
- CA-03: Information Exchagne
- SC-04: Information in Shared System Resources
- SC-07: Boundary Protection
- SC-08: Transmission Confidentiality and Integrity
- SC-11: Trusted Path
- SC-12: Cryptographic Key Establishment and Management
- SC-13: Cryptographic Protection
- SC-16: Transmission of Security and Privacy Attributes
- SC-40: Wireless Link Protection
- SC-43: Usage Restrictions
- SI-03: Malicious Code Protection
- SI-04: System Monitoring
- SI-07: Software, Firmware, and Information Integrity

CIS Controls

CIS Sub-Control	Asset Type	Security Function	Title	Description
3.10	Devices	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

https://www.cisecurity.org/controls

Encryption in transit examples:

- Sending an email, from your laptop to a 3rd party Gmail server to the person's phone you sent it to
- Or saving a document on Sharepoint - that file goes from the computer to your cloud to your colleagues
- Or typing in your password to log into a service - that's sensitive data that encryption helps to keep confidential

TLS (Transport Layer Security)

- A handshake between an end users web browser, and a back end server, establishing an encrypted session that puts a padlock beside the URL in your browser

SSH (Secure Shell)

- Typically used in the Command Line Interface (CLI) for remote management of servers and network hardware.
- Frequently used in automated scripts for remote system updates, backups and administrative tasks, or in an Integrated Development Environment (IDE) for connecting to version control systems, remote debugging and deploying applications

Encryption at rest examples:

- Operating systems
  - Bitlocker (WIndows)
  - Veracrypt (Windows, Ubuntu, macOS)
  - FileVault (macOS)
- Database encryption
  - Data files on the disk, backup files, logs
- Mobile device encryption
- Modern hard drives and solid-state drives (SSDs)

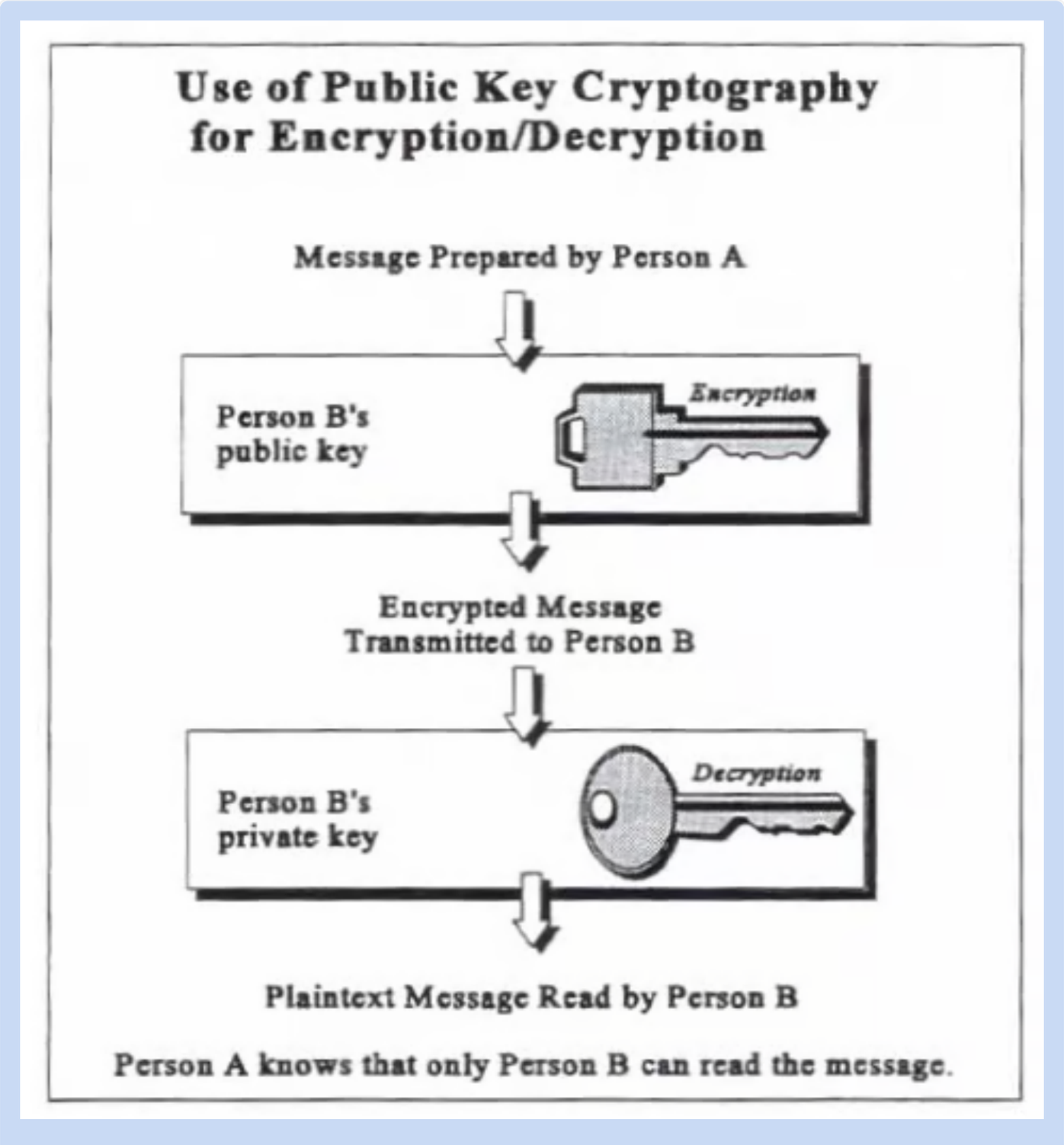
NIST SP 800-53

SC-12 Cryptographic Key Establishment and Management

- There are two main types of encryption:

Distinct Features	Symmetric (Secret Key) Cryptography	Asymmetric (Public Key Cryptography)
Number of Keys	Single Key	Pair of keys
Types of Keys	Key is secret	One key is private, and one key is public
Protection of Keys	Disclosure and modification	Disclosure and modification for private keys and modification for public keys
Relative Speeds	Faster	Slower

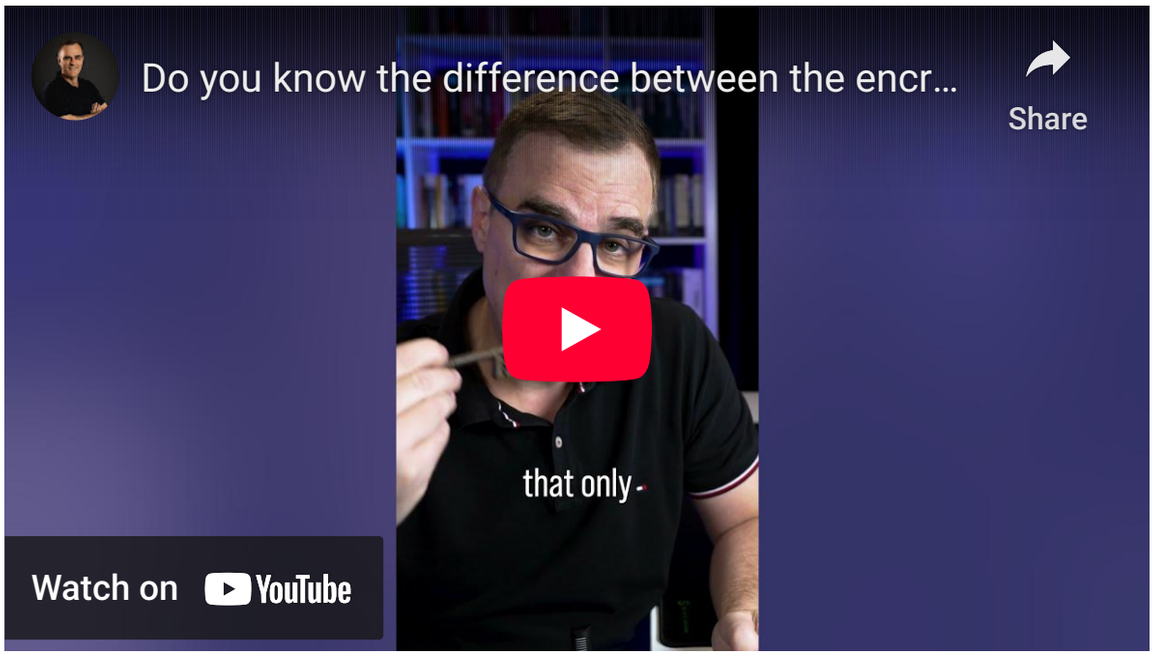
Asymmetric Encryption



NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook

Chapter 19 - Cryptography

csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter19.html



Symmetric Encryption

- Uses the same key for both encrypting and decrypting data (block cipher). This key must be shared and kept secret between the sender and the recipient
- Examples are AES (Advanced Encryption Standard) and DES (Data Encryption Standard)
- Typically faster than asymmetric encryption and is commonly used for encrypting large amounts of data
- Often used for encrypting data at rest, such as files on a hard drive, or data in transit in scenarios where secure key exchange has already occurred

SYMMETRIC KEYS

Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS- validated; NSA-approved] key management technology and processes.

Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods.

NIST SP 800-53, REV. 5

- Use of asymmetric (public key) cryptography to securely establish symmetric (shared keys) between two parties.
- Although SP 800-56A is primarily about key exchange mechanisms like Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH), the secure keys established can be used with symmetric key algorithms like AES-256 for encrypting data in transit.

1. Introduction

Many U.S. Government Information Technology (IT) systems need to employ well-established cryptographic schemes to protect the integrity and confidentiality of the data that they process. Algorithms such as the Advanced Encryption Standard (AES) as defined in Federal Information Processing Standard (FIPS) 197,[1] and the Keyed-Hash Message Authentication Code (HMAC) as defined in FIPS 198[2] make attractive choices for the provision of these services. These algorithms have been standardized to facilitate interoperability between systems. However, the use of these algorithms requires the establishment of keying material between the participating entities in advance. Trusted couriers may manually distribute this secret keying material. However, as the number of entities using a system grows, the work involved in the distribution of the secret keying material could grow rapidly. Therefore, it is essential to support the cryptographic algorithms used in modern U.S. Government applications with automated key-establishment schemes.

A key-establishment scheme can be characterized as either a key-agreement scheme or a key-transport scheme. The asymmetric-key-based key-agreement schemes in this Recommendation are based on the Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) algorithms. Asymmetric-key-based key-establishment schemes using Integer Factorization Cryptography are specified in SP 800-56B.[3] The selection of schemes specified in this Recommendation is based on standards for key-establishment schemes developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.42, *Agreement of Symmetric Keys using Discrete Logarithm Cryptography*, and ANS X9.63, *Key Agreement and Key Transport using Elliptic Curve Cryptography*.

2. Scope and Purpose

This Recommendation provides the specifications for key-agreement schemes that are appropriate for use by the U.S. Federal Government and is intended for use in conjunction with NIST Special Publication (SP) SP 800-57.[4] This Recommendation (i.e., SP 800-56A) and SP 800-57 are intended to provide sufficient information for a vendor to implement secure key establishment using asymmetric algorithms in FIPS 140[5]-validated modules.

A scheme may be a component of a protocol, which in turn provides additional security properties not provided by the scheme when considered by itself. Note that protocols, per se, are not specified in this Recommendation.

- AES is considered a “well established cryptographic scheme”
- AES is defined in FIPS-197

Table 3. Key-Block-Round Combinations

	Key length		Block size		Number of rounds
	Nk	(in bits)	*Nb*	(in bits)	*Nr*
AES-128	4	128	4	128	10
AES-192	6	192	4	128	12
AES-256	8	256	4	128	14

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

- AES-256 has the largest key length and number of rounds

FIPS-197: Advanced Encryption Standard (AES)

FIPS 197 ADVANCED ENCRYPTION STANDARD (AES)

Federal Information

Processing Standards Publication 197

Published: November 26, 2001
Updated: May 9, 2023

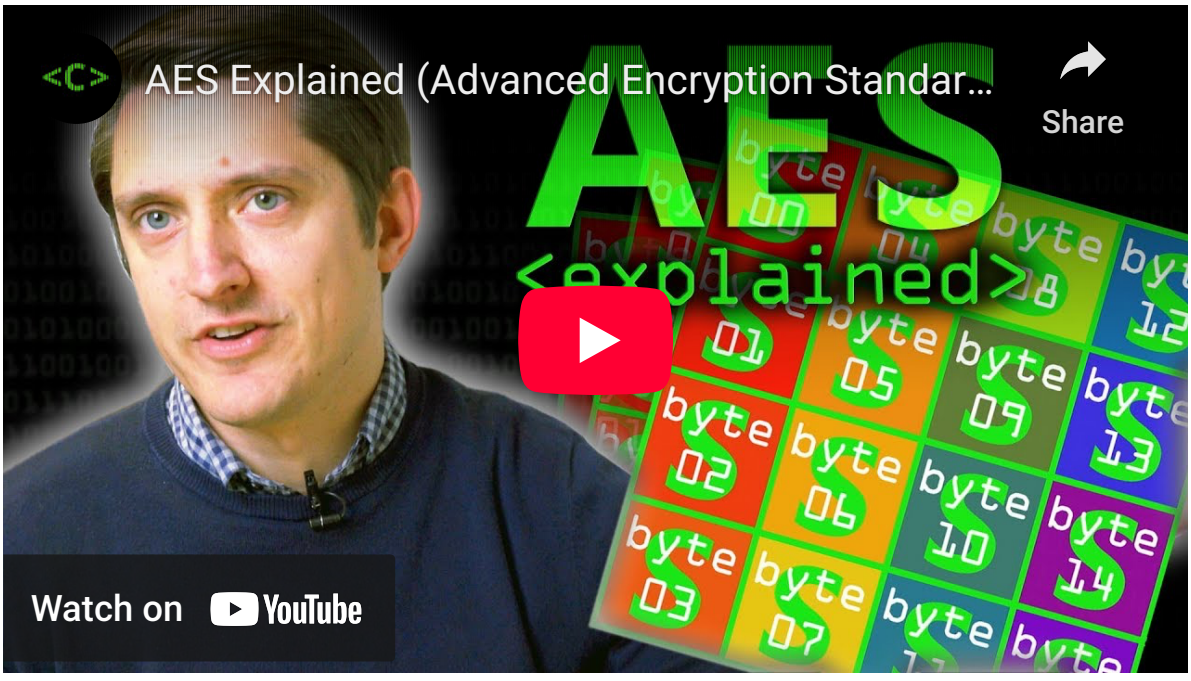
Announcing the
ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS) are developed by NIST under 15 U.S.C. 278g-3 and issued by the Secretary of Commerce under 40 U.S.C. 11331.

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS 197).
2. **Category of Standard.** Computer Security Standard, Cryptography.
3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) digital information.

   The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf



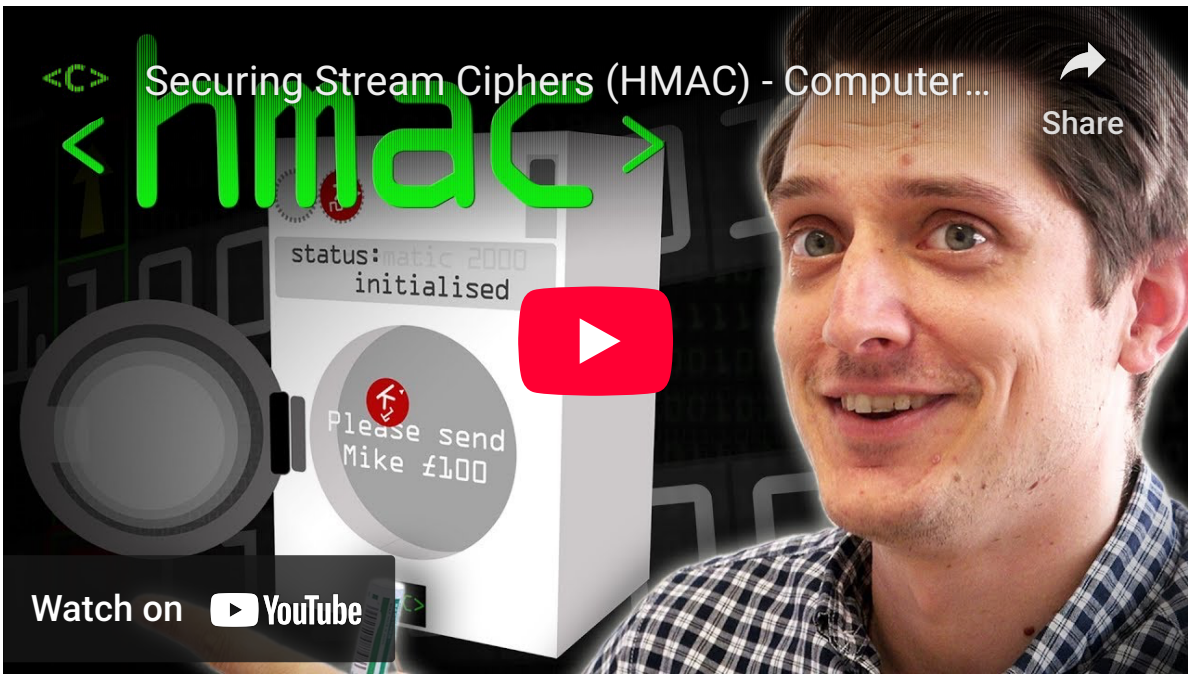
FIPS-198: The Keyed-Hash Message Authentication Code (HMAC)

- HMAC (Hash-Based Message Authentication Code) can be used in conjunction with AES (Advanced Encryption Standard) to provide both encryption and integrity protection for data in transit
- For example, in a typical TLS session, AES might be used to encrypt the data being transmitted, while HMAC is used to ensure the data integrity and authenticate that the data has not been tampered with during transit

1. INTRODUCTION

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity checks based on a secret key are usually called message authentication codes (MACs). Typically, message authentication codes are used between two parties that share a secret key in order to authenticate information transmitted between these parties. This Standard defines a MAC that uses a cryptographic hash function in conjunction with a secret key. This mechanism is called HMAC [HMAC]. HMAC shall use an Approved cryptographic hash function [FIPS 180-3]. HMAC uses the secret key for the calculation and verification of the MACs.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.198-1.pdf



SP 800-56B: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography

- Like 800-56A, it's about secure key exchange, but based on RSA encryption

methods.

- The keys established can similarly be used with symmetric encryption algorithms such as AES-256 for secure data transmission.

1. Introduction

Many U.S. Government Information Technology (IT) systems need to employ strong cryptographic schemes to protect the integrity and confidentiality of the data that they process. Algorithms such as the Advanced Encryption Standard (AES), as defined in Federal Information Processing Standard (FIPS) 197,[1] and HMAC, as defined in FIPS 198,[2] make attractive choices for the provision of these services. These algorithms have been standardized to facilitate interoperability between systems. However, the use of these algorithms requires the establishment of secret keying material that is shared in advance. Trusted couriers may manually distribute this secret keying material, but as the number of entities using a system grows, the work involved in the distribution of the secret keying material grows rapidly. Therefore, it is essential to support the cryptographic algorithms used in modern U.S. Government applications with automated key-establishment schemes.

This Recommendation provides the specifications of key-establishment schemes that are appropriate for use by the U.S. Federal Government, based on a standard that was developed by the Accredited Standards Committee (ASC) X9, Inc: ANS X9.44.[3] A key-establishment scheme can be characterized as either a key-agreement scheme or a key-transport scheme. This Recommendation provides key-agreement and key-transport schemes that are based on the Rivest Shamir Adleman (RSA) asymmetric-key algorithm.

2. Scope and Purpose

This Recommendation is intended for use in conjunction with NIST Special Publication (SP) 800-57.[4] This key-establishment Recommendation, SP 800-57, and FIPS 186[5] are intended to provide information for a vendor to implement secure key-establishment using asymmetric algorithms in FIPS 140[6] validated modules.

Note that a key-establishment scheme is a component of a protocol that may provide security properties not provided by the scheme when considered by itself; protocols, per se, are not specified in this Recommendation.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

NIST SP 800-56C: Recommendation for Key-Derivation Methods in Key-Establishment Schemes

- Key derivation methods are another crucial process that we don't want to become the weak link
- Even if AES-256 encryption is robust, the security of the encryption scheme is largely dependent on the secrecy and integrity of the keys used. If keys are derived or managed poorly, the strength of AES-256 can be undermined
- If our vendor adheres to these guidelines, it can add a layer of trust in how they handle key management

2 Scope and Purpose

This Recommendation specifies two categories of key-derivation methods that can be employed, as required, to derive keying material from a shared secret Z generated during the execution of a key-establishment scheme specified in [SP 800-56A] or [SP 800-56B].

In addition to the currently **approved** techniques for the generation of the shared secret Z as specified in SP 800-56A and SP 800-56B, this Recommendation permits the use of a "hybrid" shared secret of the form $Z' = Z || T$, a concatenation consisting of a "standard" shared secret Z that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret T that has been generated using some other method. The content, format, length, and method used to generate T must be known and agreed upon by all parties that will rely upon the derived keying material, as well as by any agents trusted to act on their behalf. The key-derivation methods specified in this Recommendation will process a hybrid Z' in the same way they process a standard Z. Therefore, for simplicity of notation and exposition, any shared secret denoted by the symbol Z in the remainder of this Recommendation can be of either the "standard" or "hybrid" variety.

The first category of specified key-derivation methods consists of a family of one-step key-derivation functions that derive keying material of a desired length from a shared secret that was generated during the execution of a key-establishment scheme (and possibly other information as well).

The second category consists of an extraction-then-expansion key-derivation procedure that involves two steps:

1) Randomness extraction, to obtain a single cryptographic key-derivation key from a shared secret generated during the execution of a key-establishment scheme.
2) Key expansion, to derive keying material of the desired length from that key-derivation key and other information. Since NIST's [SP 800-108] specifies several families of key-derivation functions that are **approved** for deriving additional keying material from a given cryptographic key-derivation key, those functions are employed in the second (key-expansion) step of these two-step procedures.

In addition to the key-derivation methods whose specifications are provided in this document, [SP 800-135][4] describes several variants (of both the one-step and two-step methods) that are **approved** for specific applications.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

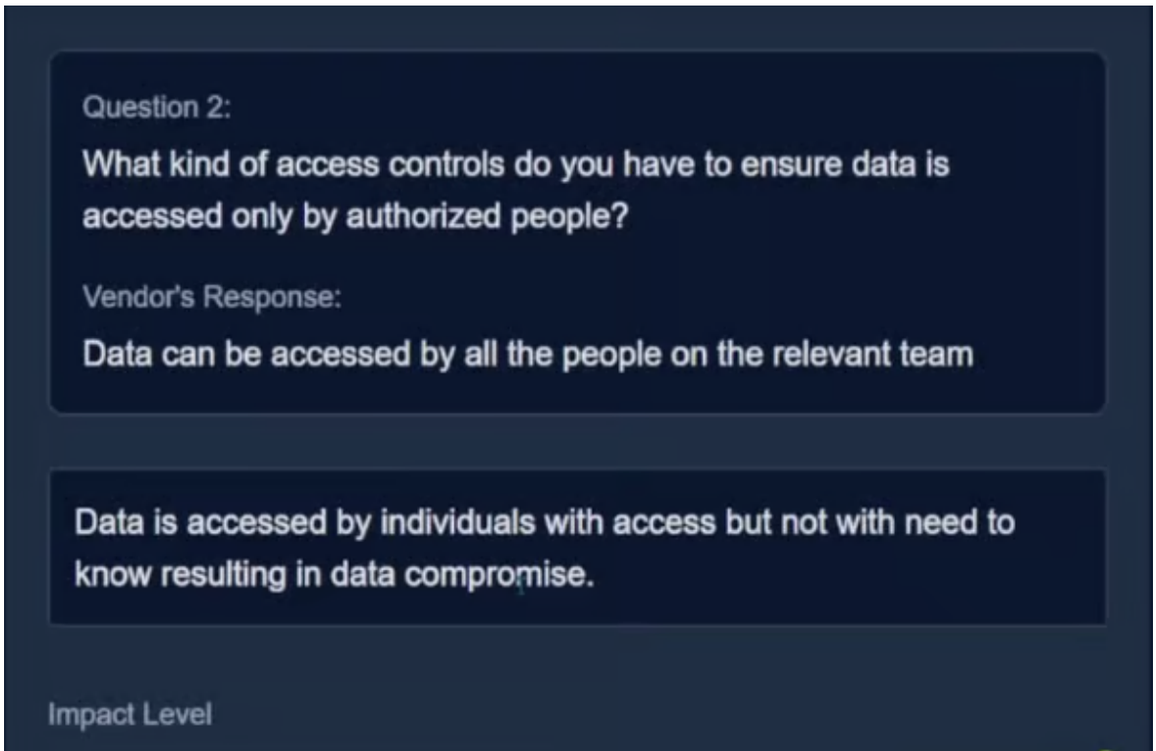
Question 2: PR.AA-05 Access Permissions | Principle of Least Privilege

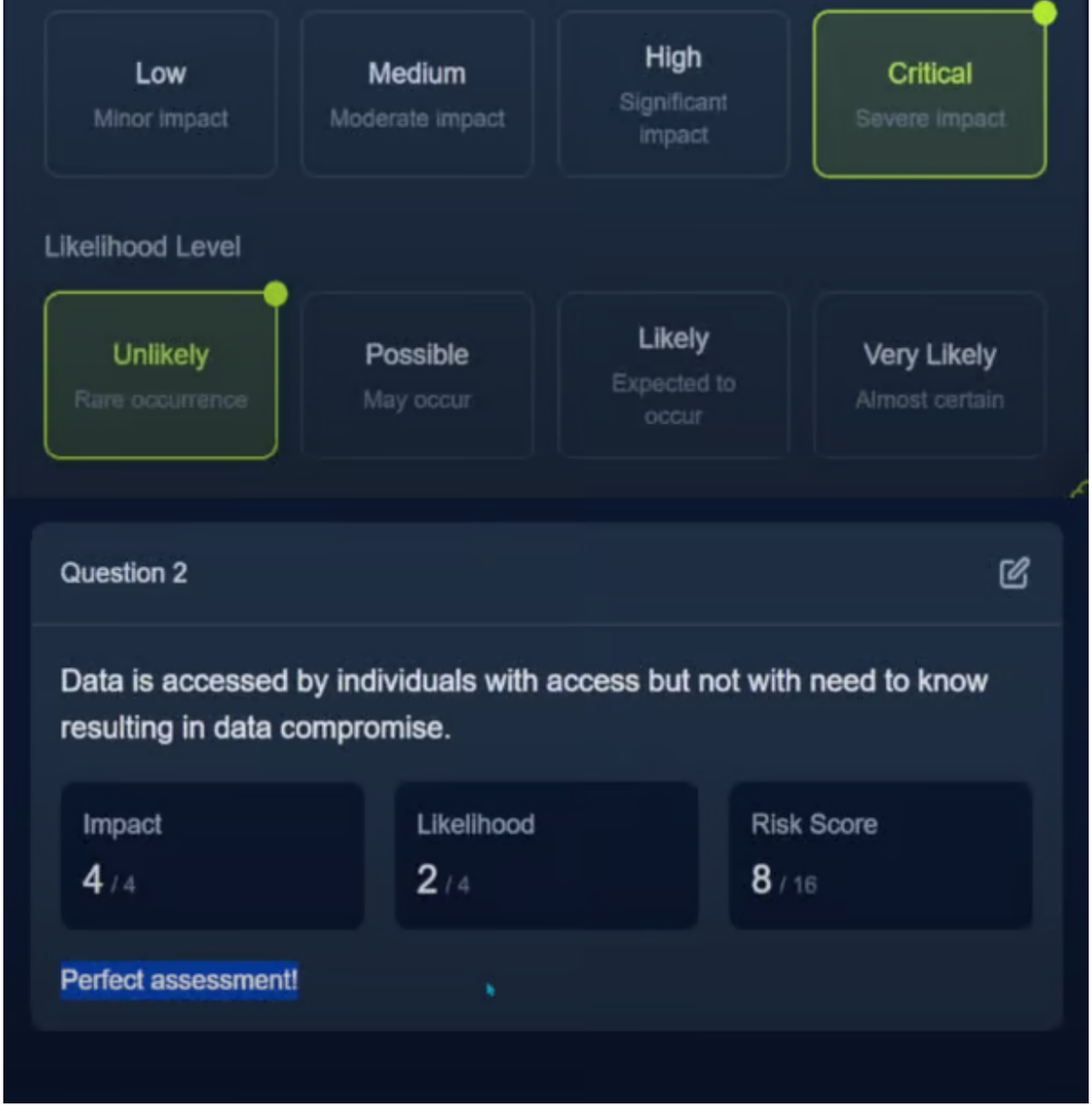
Alright, so let's go to question two: What kind of access controls do you have to ensure data is accessed only by authorized people? This is very important; access control is huge especially in a modern society where we're doing all sorts of partnering in cloud services and stuff. The vendor here, Violet Wolf, says data can be accessed by all the people on the relevant team. This is decent controls but there may be people on the team who don't really need access—so financial planner, a project manager, contractors that are supporting the team but not directly required to access the data. There is a little bit of a risk here; basically you want ideally only people with a need-to-know to have access—least use or least privilege is the control if you want to look it up in NIST 853.

The risk here is that data is accessed by individuals with access but not with need-to-know resulting in data breach or at least data compromise. Again, if people are getting access to this where they shouldn't—severe impact—this remember GRC and qualitatively assessing the impact and likelihood of a risk is very subjective; it's very fluid. This is why we have discussions about this and you're able to add additional controls to reduce or mitigate down risk levels to acceptable levels.

In this instance we'll say the impact is critical but anytime you make a decision on impact and likelihood you must absolutely be ready to defend it in a meeting because basically what you're saying is we need to invest more into security to reduce the risk to acceptable levels or you're saying we're not going to use this vendor and potentially cost this vendor millions of dollars or cost our business more money because the other vendors are more expensive. Just whenever you're choosing your values it's not just close your eyes and whack-a-mole; it's like literally you have to be able to defend this.

Dr. Gerald Auger





NIST CSF Category Lookup: PR.AA-05

CSF Subcategory ID	Implementation Example(s)
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	**Ex1**: Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed **Ex2**: Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health) **Ex3**: Restrict access and privileges to the minimum necessary (e.g., zero trust architecture) **Ex4**: Periodically review the privileges associated with critical business functions to confirm proper separation of duties

Informative References

CIS Controls v8.0:

CIS Sub-Control	Asset Type	Security Function	Title	Description
3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

SP 800-53 Rev 5.1.1:

- AC-01: Access Control Policy and Procedures
- AC-02: Account Management
  - Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. [Assignment: organization-defined attributes (as required)];
- AC-03: Access Enforcement
  - Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject.
- AC-05: Separation of Duties
- AC-06: Least Privilege
  - Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
- AC-10: Concurrent Session Control
- AC-16: Security and Privacy Attributes
- AC-17: Remote Access
- AC-18: Wireless Access
- AC-19: Access Control for Mobile Devices
- AC-24: Access Control Decisions

Question 3: *ID.AM*-8 Data Lifecycle | Securely Dispose of Data

Okay so now let's go to question three: How long do you keep client data after the case is closed? This is a data governance issue—a data retention issue—more than a month is not good; they shouldn't be keeping it longer than they need to.

Data breach—retaining data longer than needed can result in data compromise through a data breach. Honestly you see this all the time with third-party data breaches—literally all the time—and it stinks because typically the business like our business in this case would be the one getting raked through the news and the mud—not the company that held our data. Go look at like the Snowflake breach recently or go look at what CL0P ransomware did with Progress MOVEit software last summer—you know what I mean? The companies that are impacted are not the ones that actually had the data breach.

This is literally the risk we're trying to deal with—significant impact—it would be really bad frankly; it wouldn't jeopardize catastrophic business operations but it would be a pretty high impact. More than a month—I mean you're basically dancing with fire so I'm going to say expected to occur.

Dr. Gerald Auger

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Question 3:

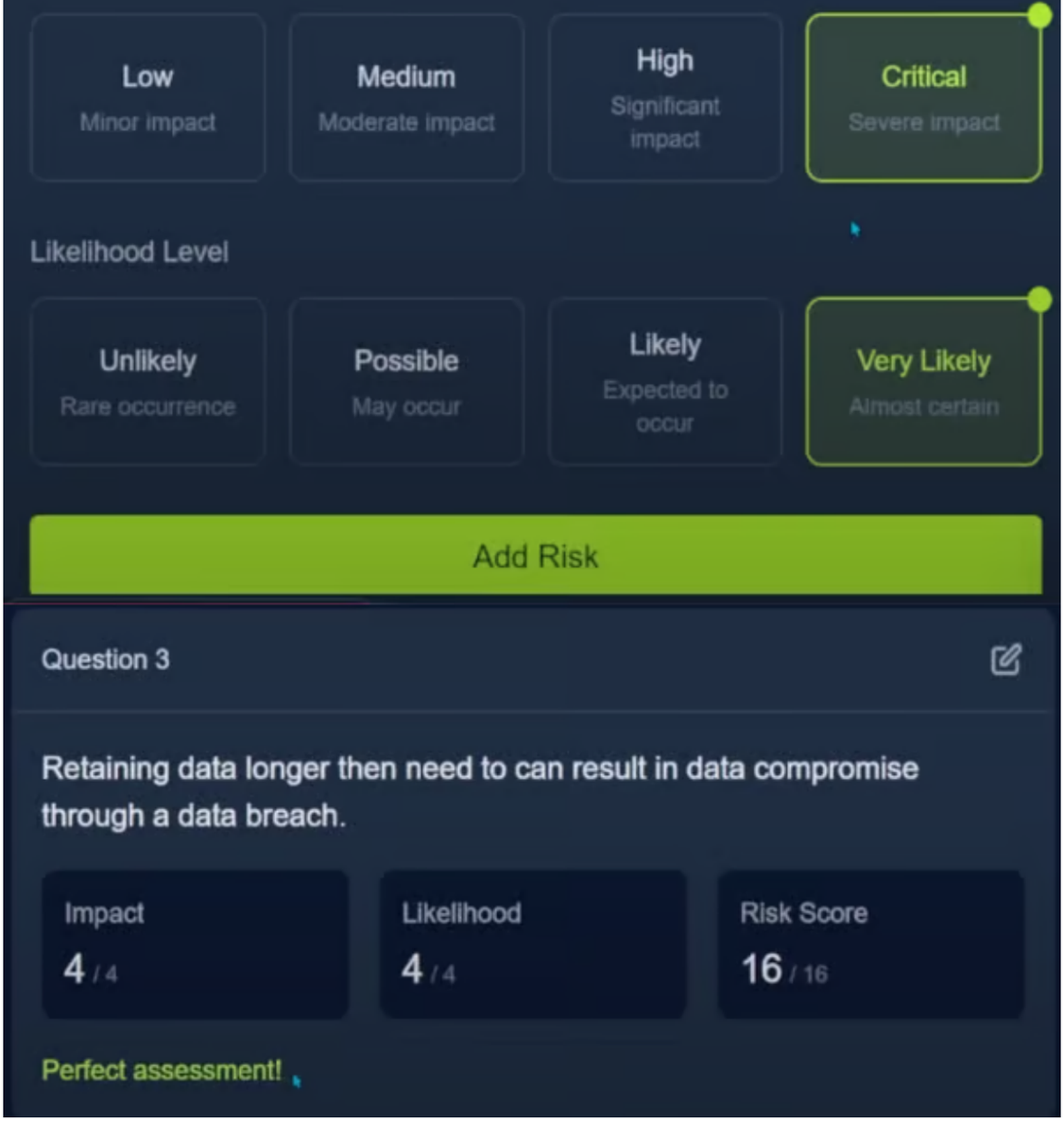
How long do you keep client data after the case is closed?

Vendor's Response:

More than 1 month

Retaining data longer then need to can result in data compromise through a data breach.

Impact Level



CIS Sub-Control	Asset Type	Security Function	Title	Description
3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

NIST CSF Category Lookup: ID.AM-08

CSF Subcategory ID	Implementation Example(s)
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	Ex7: Securely destroy stored data based on the organization's data retention policy using the prescribed destruction method, and keep and manage a record of the destructions

Informative References

CIS Controls v8.0: 1.1 CIS Controls v8.0: 3.5

CIS Sub-Control	Asset Type	Security Function	Title	Description
3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

SP 800-53 Rev 5.1.1:

- CM-09: Configuration Management Plan
- CM-13: Information System Monitoring Plan
  - Control: Develop and document a map of system data actions.
  - Discussion: Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal.
- MA-02: Controlled Maintenance
- MA-06: Timely Maintenance
- PL-02: System Security Plan
- PM-22: Personally Identifiable Information Quality Management
- PM-23: Data Governance Body
  - A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements.
- SA-03: System Development Life Cycle
- SA-04: Acquisition Process
- SA-08: Security Engineering Principles
- SA-22: Unsupported System Components
- SI-12: Information Management and Retention
  - Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information.
- SI-18: Personally Identifiable Information Quality Operations
- SR-05: Acquisition Strategies, Tools and Methods
- SR-12: Component Disposal bankofamerica.com

Contains Search Done

California Consumer Privacy Act Notice

How Long We Retain Personal Information

The length of time that we intend to retain each category of Personal Information will depend on several criteria, including (i) the length of time we are required to retain Personal Information in order to comply with applicable legal and regulatory requirements, (ii) the length of time we may need to retain Personal Information in order to accomplish the business or commercial purpose(s) for which such Personal Information is collected, used or disclosed (as indicated in this Notice), and (iii) whether you choose to exercise your right, subject to certain exceptions, to request deletion of your Personal Information.

Sale or Sharing of Personal Information

In the 12 months preceding the date of this Notice, we have not "sold" or "shared" Personal Information or Sensitive Personal Information subject to the CCPA nor have we "sold" or "shared" Personal Information or Sensitive Personal Information of minors under the age of 16.

For purposes of this Notice:

https://www.bankofamerica.com/security-center/ccpa-disclosure/

facebook.com

Privacy Center

- Privacy Center home
- Search
- Privacy topics
- More privacy resources
- Privacy Policy
  - What is the Privacy Policy and what does it cover?
  - What information do we collect?
  - How do we use your information?
  - How is your information shared on Meta Products or with integrated partners?

How long do we keep your information?

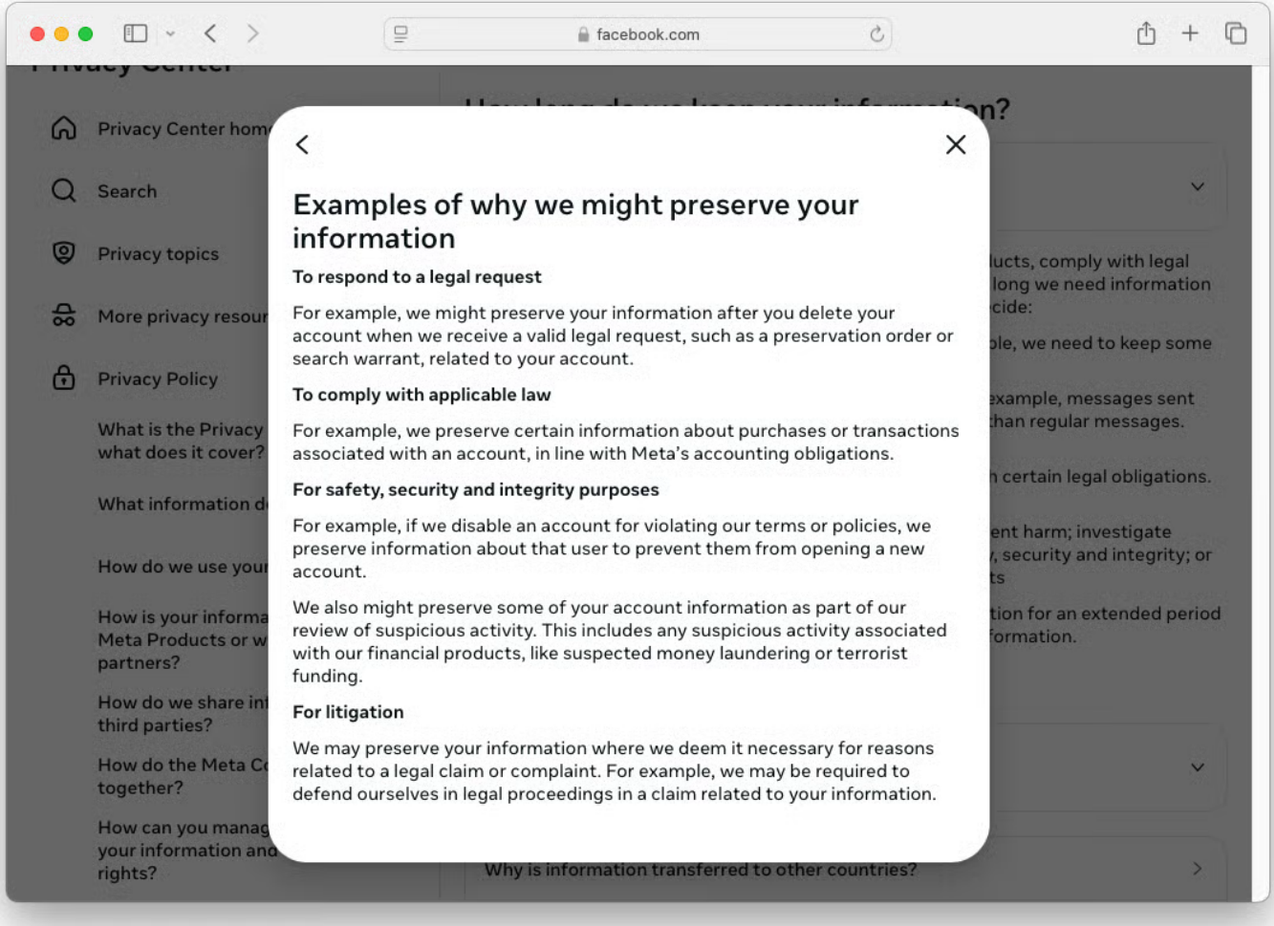
Highlights

We keep information as long as we need it to provide our Products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis. Here's what we consider when we decide:

- If we need it to operate or provide our Products. For example, we need to keep some of your information to maintain your account. Learn more.
- The feature we use it for, and how that feature works. For example, messages sent using Messenger's vanish mode are retained for less time than regular messages. Learn more.
- How long we need to retain the information to comply with certain legal obligations. See some examples.
- If we need it for other legitimate purposes, such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our rights, property or products

In some instances and for specific reasons, we'll keep information for an extended period of time. Read our Policy about when we may preserve your information.

https://www.facebook.com/privacy/policy/



Conclusion: Crushed it! 🥊

Nice job everybody! Learn more about GRC risk management visiting the risk management room at TryHackMe. Let's go ahead and hit complete alright - absolutely crushed it! Hope you enjoyed day nine of Advent of Cyber. I'm Gerry from Simply Cyber, I'll see you tomorrow.

Dr. Gerald Auger

Keep reading

Why Careers in Cybersecurity GRC are Underrated: Rant Part 2

Steve McMichael /

You Need To Study GRC Engineering, Right Now!

Steve McMichael /

The Untapped Potential of Business Skills in Cybersecurity Governance,...

Breaking into cybersecurity from a business background is not only possible, but valuable

Steve McMichael /

View more ›

© 2025 CPA to Cybersecurity Privacy policy Terms of use

Powered by