CISSP EXAM CRAM
THE COMPLETE COURSE

GET CERTIFIED FAST!

Coverage of all 8 domains

Strategy guidance

Proven learning techniques

with **Pete Zerger** vCISO, CISSP, MVP

WHO AM I?

Cybersecurity Strategist

vCISO for a regional bank

Speaker and Author

16-time Microsoft MVP

LinkedIn Learning Instructor

Content Developer (YouTube)

INSIDE CLOUD AND SECURITY

Pete Zerger

CISSP, vCISO, MVP


MORE IMPORTANTLY...
Last year, I helped thousands achieve cybersecurity certifications, including CISSP
Pete Zerger
CISSP, vCISO, MVP

ABOUT CISSP EXAM CRAM VIDEOS

GOAL: To help you get **further**, ***faster*** in your CISSP exam prep!

This series gets right to the point and eliminates the fluff!

Focuses on key characteristics of each concept to help you identify right (and wrong) answers on exam day.

Content utilizes several proven learning methods to accelerate your learning.

I will share techniques you can apply in your study

PACE

I intentionally speak at 115-125 words a minute.

If English is not your first language, this may be perfect!

If English is your 1st language, 1.25x may be better for you.

ABOUT CISSP EXAM CRAM VIDEOS

GOAL: To help you get **further**, ***faster*** in your CISSP exam prep!

High probability exam topics

High difficulty concepts

Frequent sources of questions

Areas that require process memorization

I want to direct your focus to high probability and high difficulty topics to optimize your prep!

INTRODUCTION: SERIES OVERVIEW

Lessons in this video:

Exam prep strategy

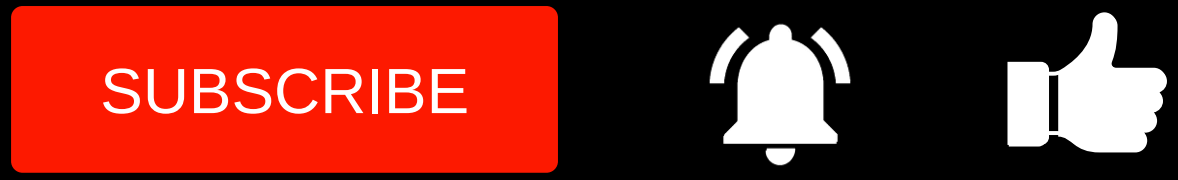
Domains 1-8

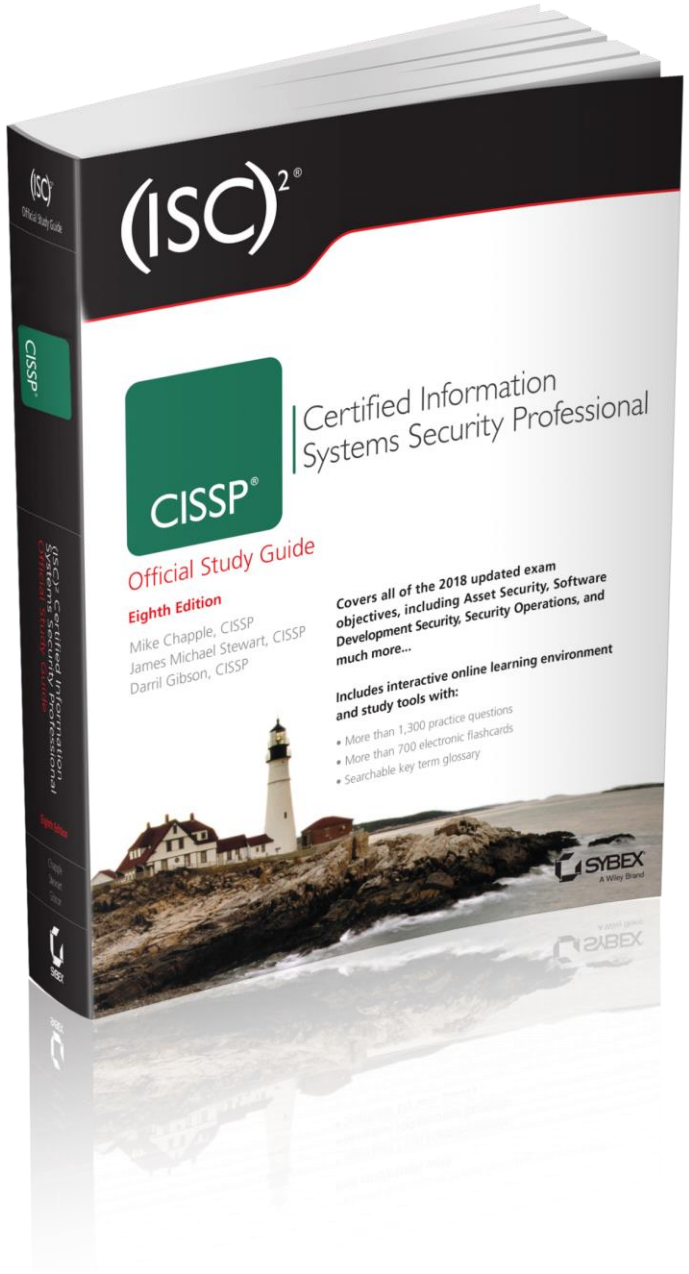
...I will also offer a few separate, shorter videos to drill down on what students report to be the most challenging areas!

Table of contents in the video description

so you can skip ahead to topic of your choice!

A pdf copy of the presentation is available in the video description!





CISSP

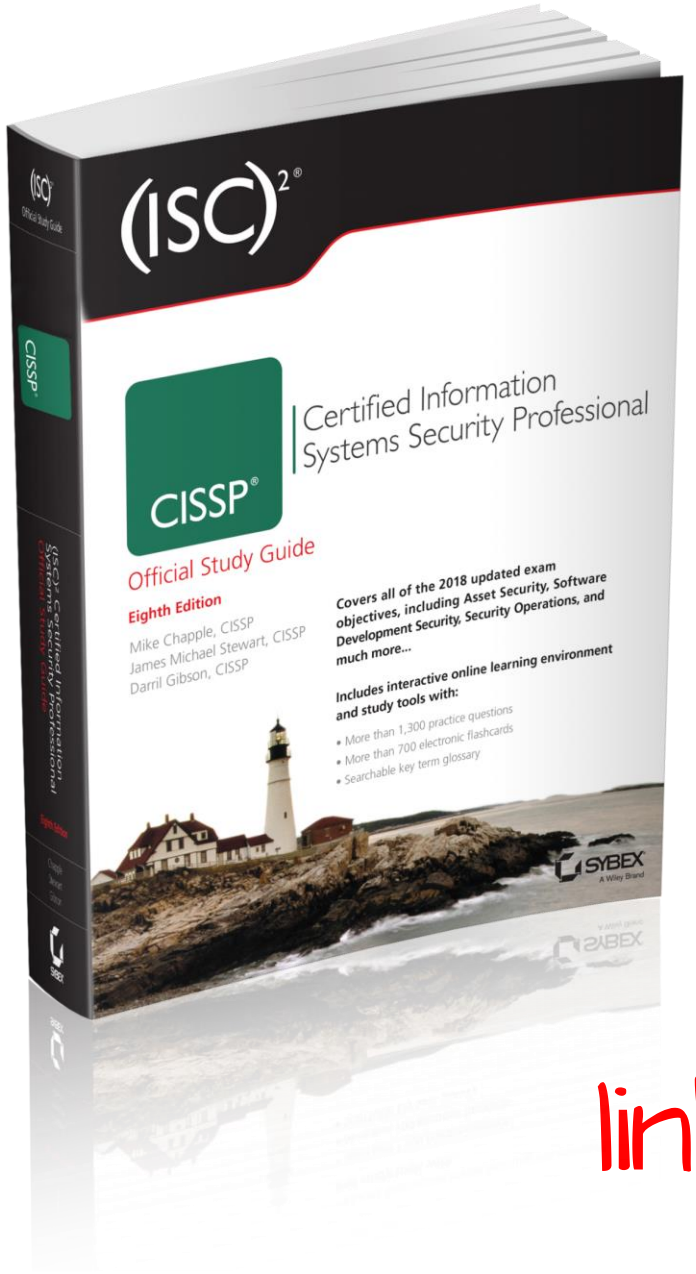
EXAM STUDY GUIDE

9th edition, electronic version

1,000 practice questions

1,000 flashcards

searchable key terms



CISSP

EXAM STUDY GUIDE

9th edition, electronic version

Buy now at amazon

link in the video description!

CISSP EXAM CRAM

THE COMPLETE COURSE

Link to additional resources, FAQs, exam updates, and errata in the description beneath the video

INSIDE CLOUD AND SECURITY


When choosing your answers...
THINK LIKE A
MANAGER
short version

DUE DILIGENCE vs DUE CARE

Due Diligence | practicing the activities that maintain the due care effort.

Due Care | doing what a reasonable person would do in a given situation. It is sometimes called the “prudent man” rule.

Together, these will reduce senior management’s **culpability & (downstream) liability** when a loss occurs.

Decision

Research
Planning
Evaluation

Implementation
Operation (upkeep)
Reasonable measures

INCREASES understanding and **REDUCES** risk

"PRUDENT MAN" RULE

Largely before the decision

DUE DILIGENCE

Doing after the decision

DUE CARE

BEFORE

Decision

Think **BEFORE** you act!

Do Detect

DUE DILIGENCE

AFTER

Actions speak louder than words

Do Correct

DUE CARE

BEFORE

Decision

AFTER

EXAMPLES

Knowledge and research of:

- ✓ Laws and Regulations
- ✓ Industry standards
- ✓ Best practices

EXAMPLES

Delivery or execution including:

- ✓ Reporting security incidents
- ✓ Security awareness training
- ✓ Disabling access in a timely way

DUE DILIGENCE

DUE CARE

KNOW YOUR PRIORITIES

Roles & Risks

YOU ARE HERE!

CISO

IT Director or Manager

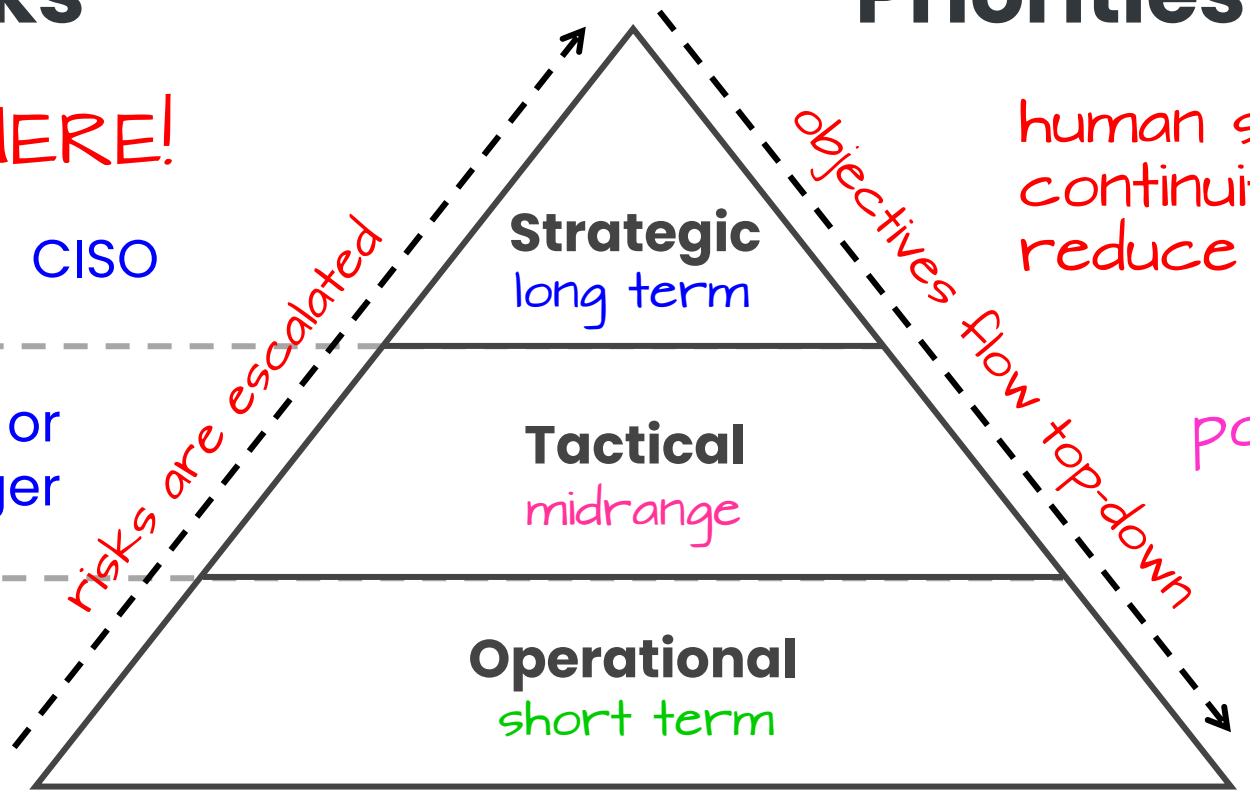
IT Engineer

Priorities & Objectives

human safety, business continuity, protect profits, reduce liability & risk

policy and planning

implement and operate



Security Planning Horizons

DON'T TOUCH, ADVISE!

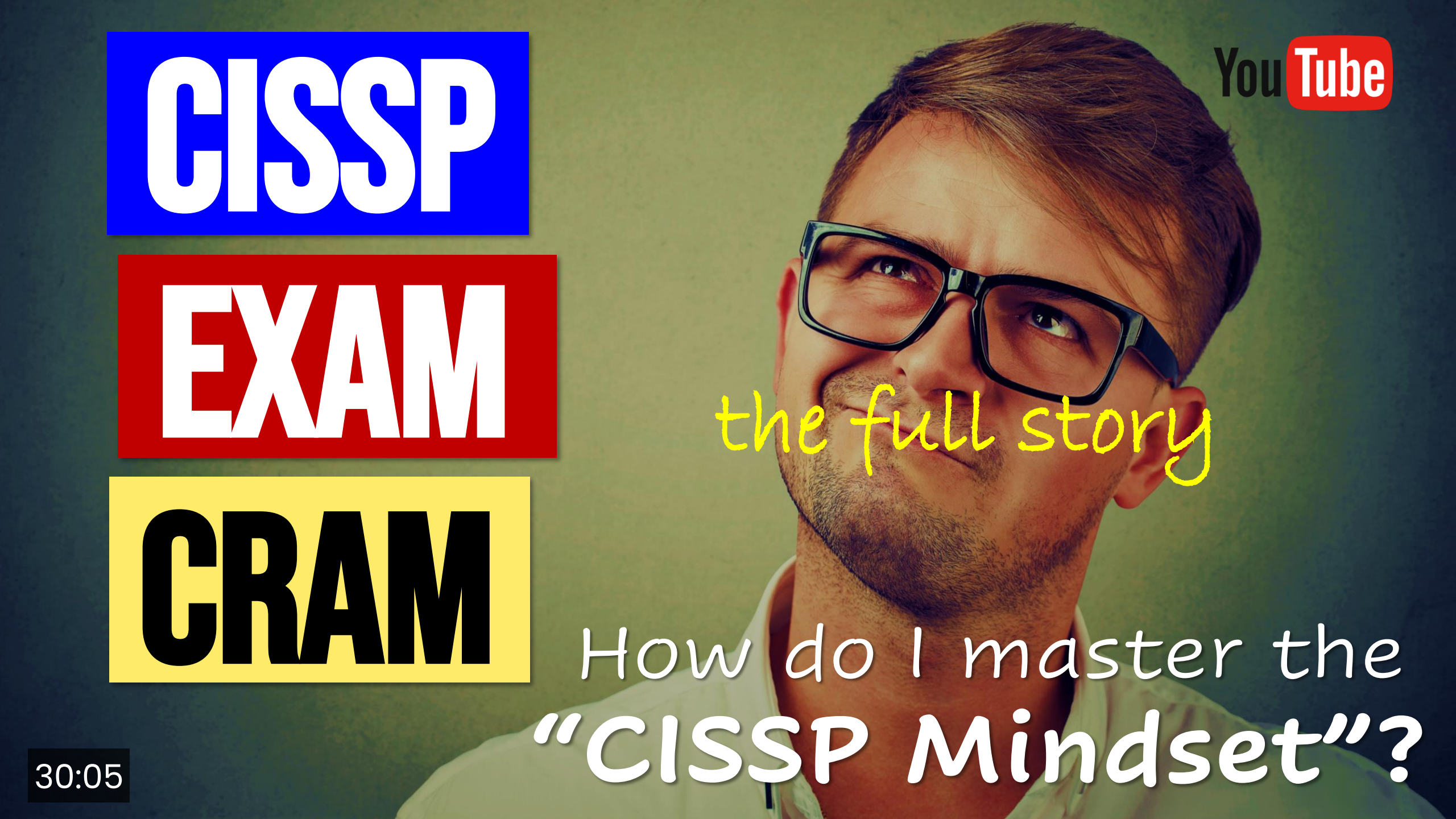
During the exam, think of yourself as an outside security consultant advising an organization

DON'T TOUCH, ADVISE!

During the exam, think of yourself as an outside security consultant advising an organization

You are advising on strategy, priorities, and safety, not doing!

Brings focus to process, role, due diligence and due care


CISSP
EXAM
CRAM
YouTube
the full story
How do I master the
"CISSP Mindset"?
30:05

CISSP EXAM CRAM

THE COMPLETE COURSE

EXAM PREP STRATEGY

INSIDE CLOUD AND SECURITY


There is no
AWARD
for the longest
STUDY TIME!

HOW LONG DOES IT TAKE TO MEMORIZE ANYTHING?

TO MEMORIZE QUICKLY

1st repetition	Right after learning
2nd repetition	After 20-30 min
3rd repetition	After 1 day
4th repetition	After 2-3 weeks
5th repetition	After 2-3 months

TO MEMORIZE FOR A LONG TIME

1st repetition	Right after learning
2nd repetition	After 15-20 min
3rd repetition	After 6-8 hours
4th repetition	After 24 hours
5th repetition	After 48 hours

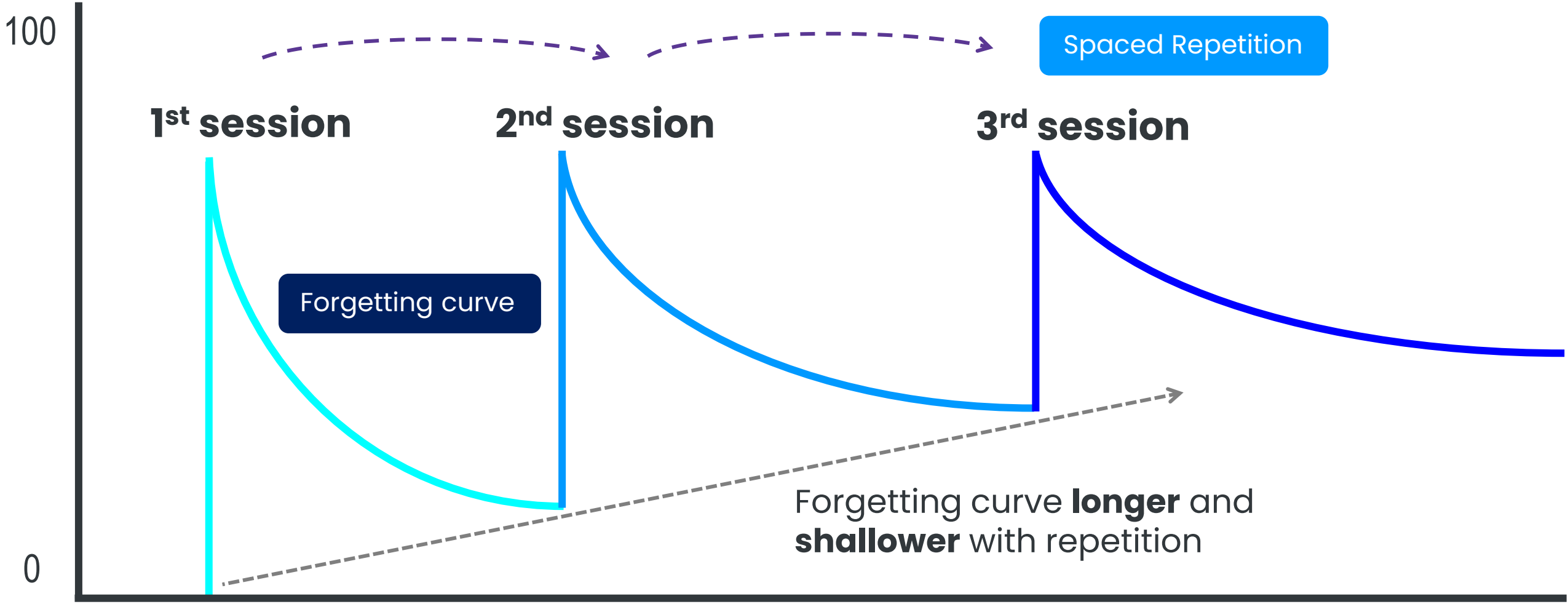
20 min

24 hours

1 week

THE POWER OF REPETITION

SPACED REPETITION



SPACED REPETITION

TO MEMORIZE QUICKLY

1st repetition	Right after learning
2nd repetition	After 20-30 min
3rd repetition	After 1 day
4th repetition	After 2-3 weeks
5th repetition	After 2-3 months

TO MEMORIZE FOR A LONG TIME

1st repetition	Right after learning
2nd repetition	After 15-20 min
3rd repetition	After 6-8 hours
4th repetition	After 24 hours
5th repetition	After 48 hours

UNDERSTANDING CONCEPTS

Studies show understanding **BEFORE** you memorize greatly improves retention

MNEMONIC DEVICE

or **memory device**, is a learning technique that makes memorizing information easier

MNEMONIC DEVICE

A common technique is the **expression mnemonic** aka an **acronym**

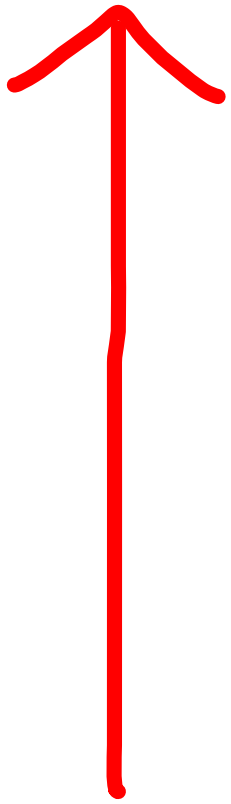
MNEMONIC DEVICE

The best mnemonic devices are **simple**, **relevant**, and **visual**

MNEMONIC DEVICE

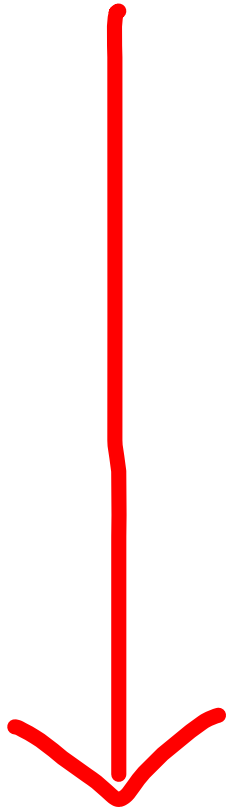
We'll start with an example using a **first letter mnemonic**

THE OSI MODEL



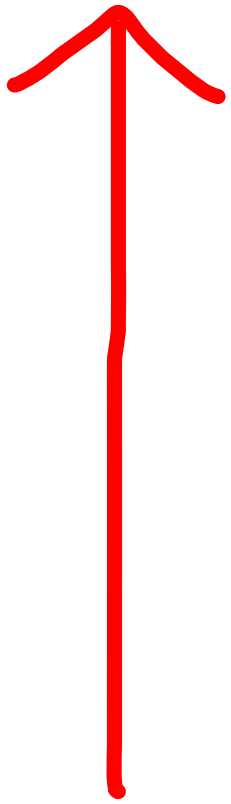
Away
Pizza
Sausage
Throw
Not
Do
Please

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



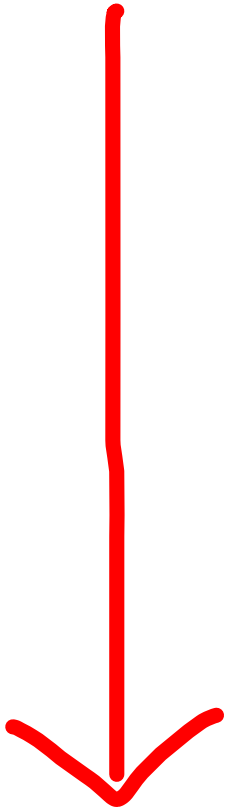
All
People
Seem
To
Need
Data
Processing

THE OSI MODEL



Aside
Processes
Security
Toss
Not
Do
Please

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



All
People
Seem
To
Need
Data
Processing

INCIDENT MANAGEMENT FRAMEWORK

1	**D**etection
2	**R**esponse
3	**M**itigation
4	**R**eporting
5	**R**ecovery
6	**R**emediation
7	**L**essons Learned

DRMRRRL

INCIDENT MANAGEMENT FRAMEWORK

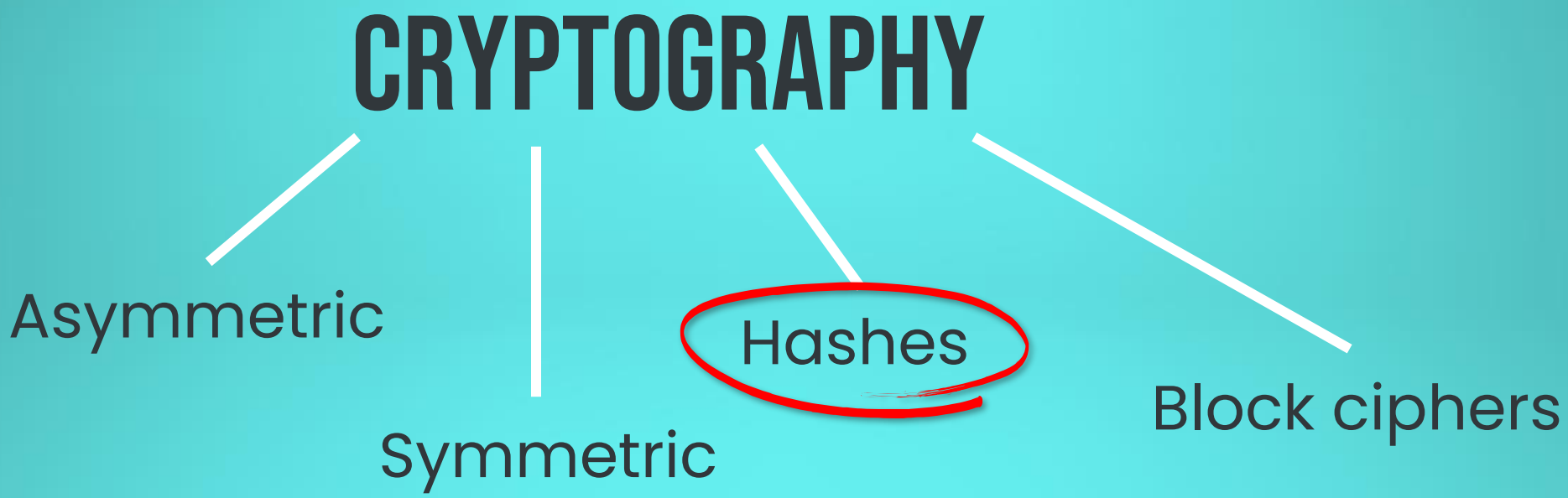
1. **D**etection
2. **R**esponse
3. **M**itigation
4. **R**eporting
5. **R**ecovery
6. **R**emediation
7. **L**essons Learned

DRMRRRL

MNEMONIC DEVICE

Chunking is a technique of breaking info into smaller pieces that make sense

CHUNKING



break into "chunks" based on a unique property

CRYPTOGRAPHY

Hash Algorithms

MD*

Message Digest

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

CRYPTOGRAPHY

Hash Algorithms

MD*

Message Digest

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

CRYPTOGRAPHY

Hash Algorithms

MD*

Message Digest

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	**NO**	MD6, et. Al.
MD4	Hash	128	**NO**	MD6, et. Al.
MD5	Hash	128	**NO**	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

CRYPTOGRAPHY

Hash Algorithms

SHA*

Secure Hash Algorithm

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

CRYPTOGRAPHY

Hash Algorithms

SHA*

Secure Hash Algorithm

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

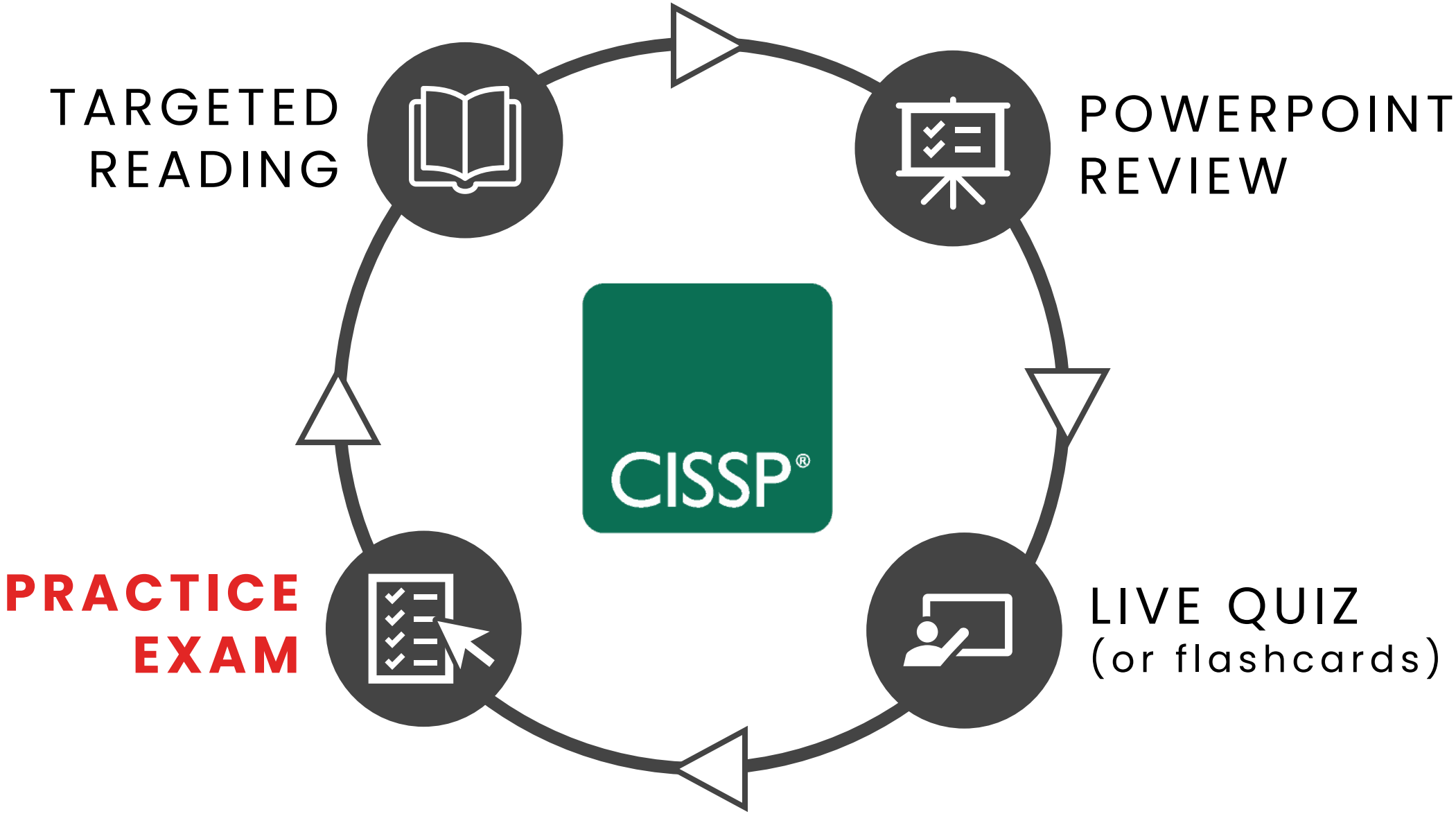
CRYPTOGRAPHY

Hash Algorithms

SHA*

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Very Strong	-
HAVAL	Hash	128, 160, 192, 224, 256		
MD2	Hash	128	No	MD6, et. al.
MD4	Hash	128	No	MD6, et. al.
MD5	Hash	128	No	MD6, et. al.
SHA-1	Hash	160	**NO**	SHA-2
SHA-224*	Hash	224	**YES**	-
SHA-256*	Hash	256	**YES**	-
SHA-384*	Hash	384	**YES**	-
SHA-512*	Hash	512	**YES**	-

80/20 STRATEGY



HOW

to best use the

PRACTICE QUIZZES

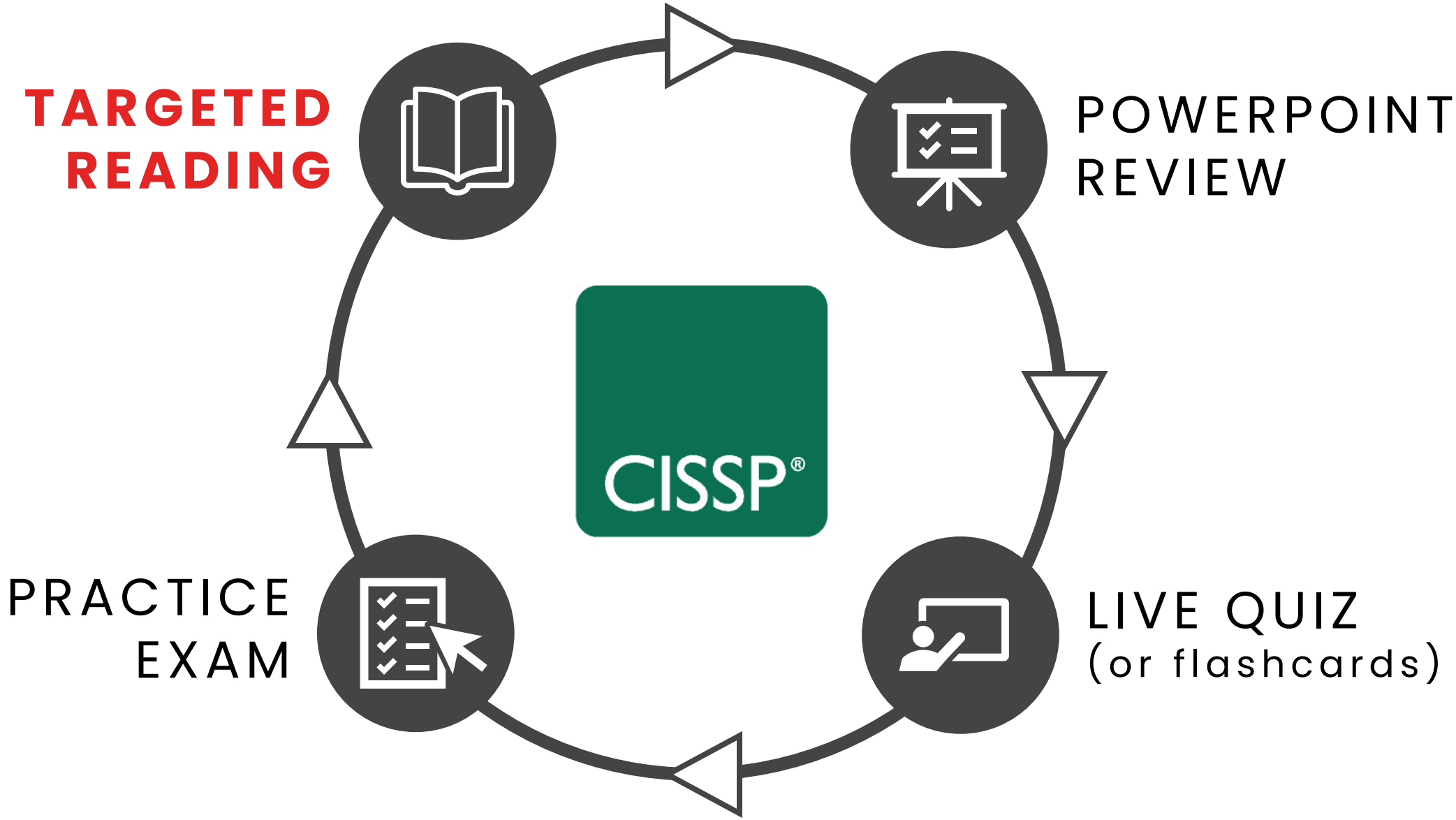
to assess your

EXAM READINESS?

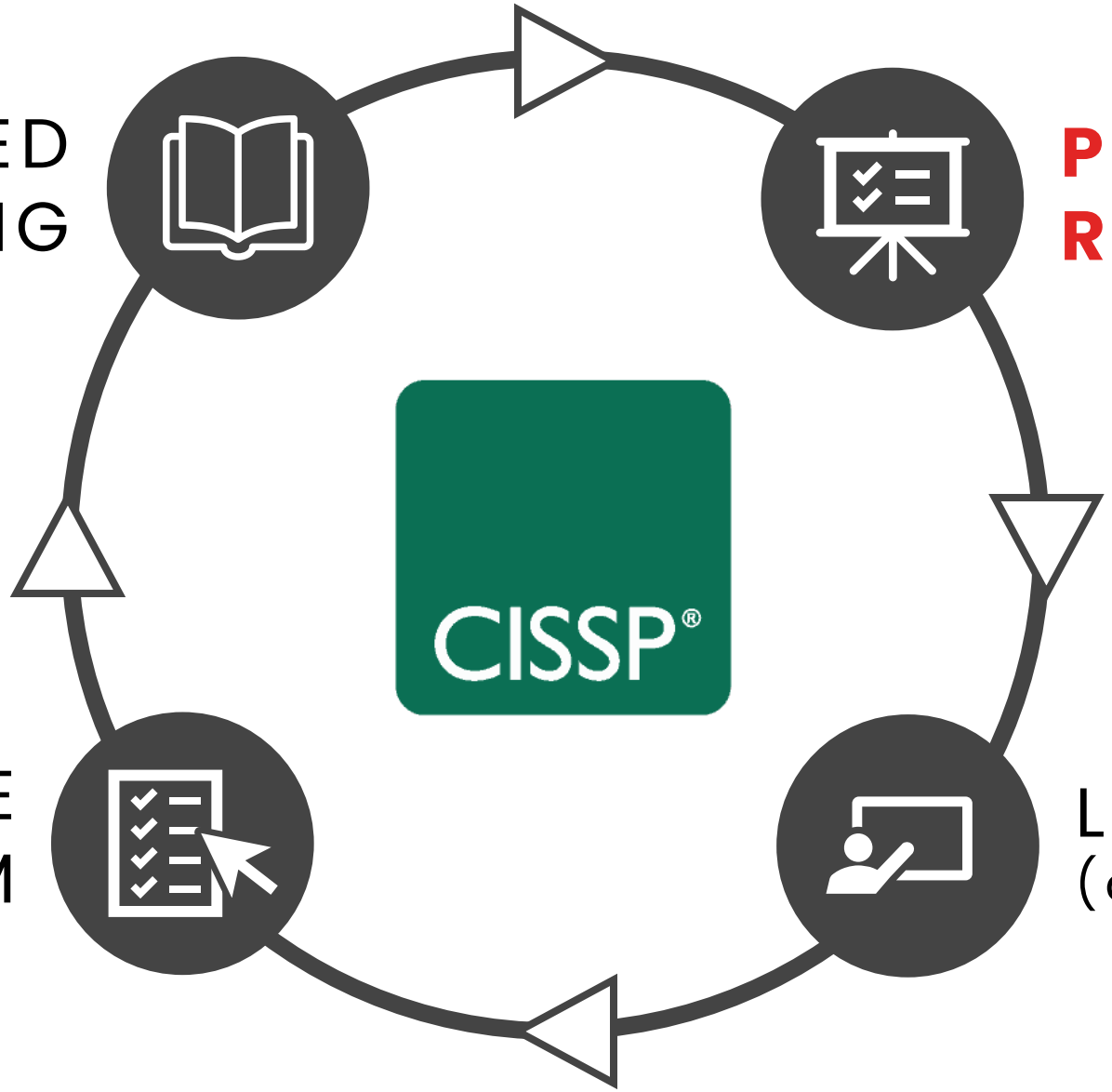
STUDY GUIDE: CHAPTER-TO-DOMAIN MAPPINGS

DOMAIN	CHAPTERS
1. Security and Risk Management	1 - 4
2. Asset Security	5
3. Security Architecture and Engineering	6 – 10
4. Communication and Network Security	11 – 12
5. Identity and Access Management	13 – 14
6. Security Assessment and Testing	15
7. Security Operations	16 – 19
8. Software Development Security	20 - 21

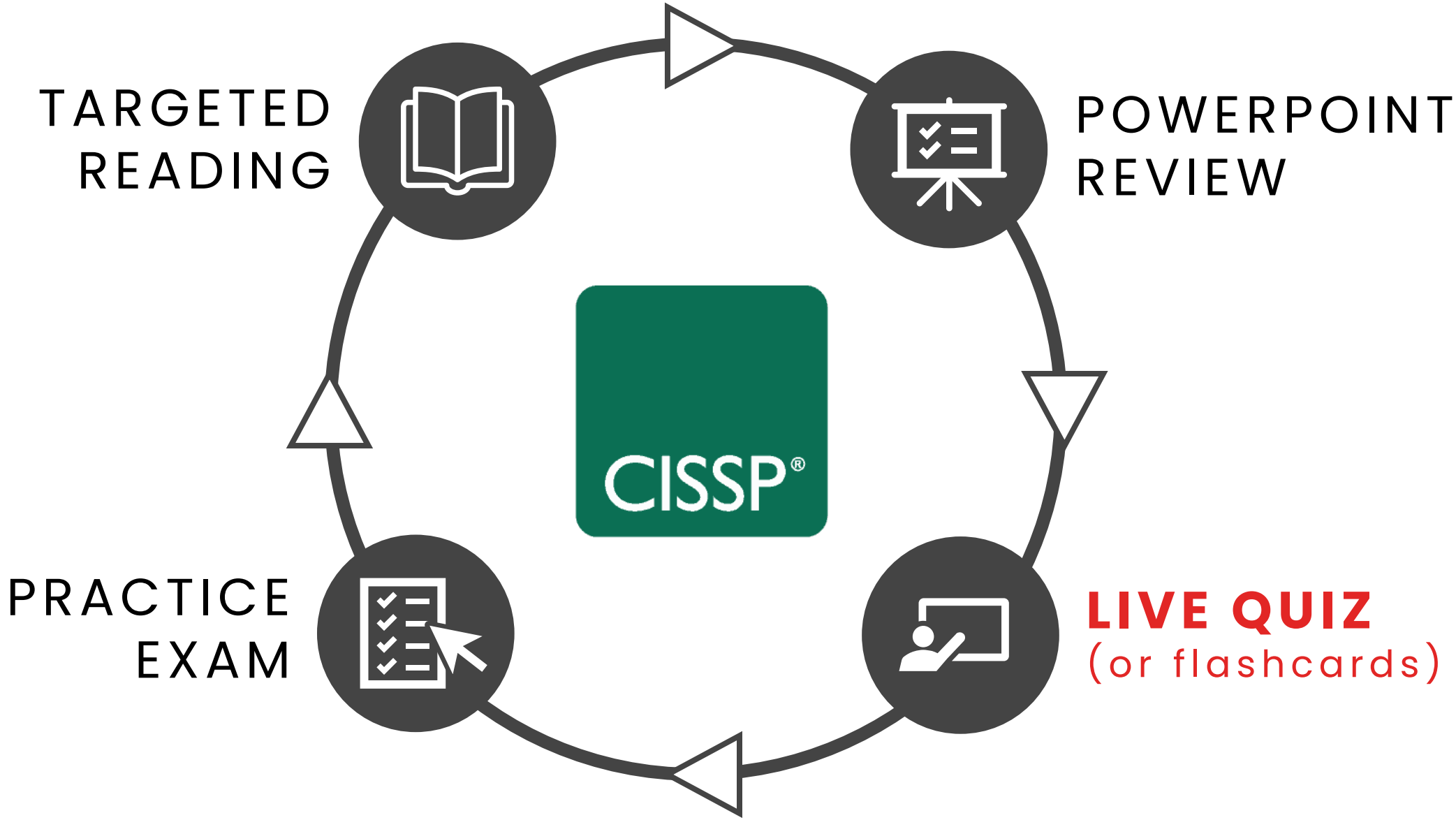
80/20 STRATEGY



80/20 STRATEGY



80/20 STRATEGY



USE MULTIPLE SOURCES

TARGETED READING

PRACTICE EXAM

LIVE QUIZ
(or flashcards)

POWERPOINT REVIEW

VIDEO CONTENT

CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 1

Security and Risk Management

INSIDE CLOUD AND SECURITY

INTRODUCTION: CISSP EXAM DOMAINS

DOMAINS	2018	2021
1. Security and Risk Management	15%	15%
2. Asset Security	10%	10%
3. Security Architecture and Engineering	13%	13%
4. Communication and Network Security	14%	**13%**
5. Identity and Access Management	13%	13%
6. Security Assessment and Testing	12%	12%
7. Security Operations	13%	13%
8. Software Development Security	10%	**11%**

NEW IN 2021 – A SUMMARY

The new syllabus for CISSP 2021 is not much different from the earlier version of 2018.

1. **NO CHANGE** in **EXPERIENCE REQUIREMENTS**
2. **NO CHANGE** in **NUMBER OF DOMAINS**

(content in some domains has been expanded)

3. **ALMOST NO CHANGE** in **DOMAIN WEIGHTS**
4. **NO MAJOR CHANGE** in **LINEAR EXAM INFORMATION**
5. **NO CHANGE** in **CAT EXAM DETAILS**

A few new topics have been introduced in some of the domains to keep up with the changing times.

ABOUT THE CAT EXAM FORMAT

3 hours, 100-150 Questions

Adapts based on your answer

Aims for 50-50 probability

Answers are final! No going back

Many think this makes the CAT exam more difficult!

ABOUT THE CAT EXAM FORMAT

70% to pass the exam

Some questions are not scored

Only pass/fail reported

Fail even 1 domain, fail the exam!

CHANGE TO THE CAT EXAM

starting June 1!

current CISSP CAT exam contains
25 pretest (unscored) items

25 more items will be added,
bringing total to 50 pretest items

Exam now 4 hours, 125-175 Questions

No other changes to syllabus or content

Some key areas:

Understand **risk** and apply **risk analysis** process

Threat modeling concepts and processes

Compliance, **legal, regulatory**, and **privacy**

Professional ethics – Know the ISC^2 code by heart

Security governance principles (ITIL, oversight)

Security policies, **standards**, **procedures** and **guidelines** (know “suggested” vs. “mandatory”)

WHAT'S NEW IN DOMAIN 1 IN 2021?

1.1 Understand, adhere to, and promote professional ethics

This is a non-event.

KNOW CIA BY HEART!

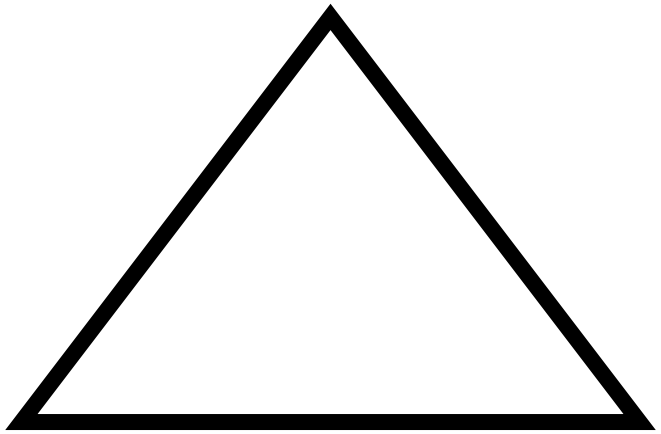
Confidentiality

Integrity

Availability

1

Confidentiality

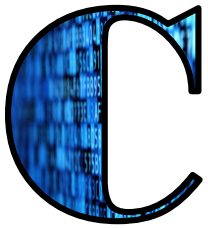


2

Integrity

3

Availability

 onfidentiality

Access controls help ensure that only authorized subjects can access objects

 ntegrity

Ensures that data or system configurations are not modified without authorization

 vailability

Authorized requests for objects must be granted to subjects within a reasonable amount of time

Memorize the ISC² code of ethics

1. **Protect** society, the commonwealth, and the infrastructure
2. **Act** honorably, honestly, justly, responsibly, and legally
3. **Provide** diligent and competent service to principals
4. **Advance** and protect the profession

There are **four levels** of **security policy development**:

Security procedures
Detailed step-by-step

Security guidelines
Offer recommendations

Security baselines
define “minimum levels”

Acceptable use policy
Assign roles and responsibilities

FOR THE EXAM

When developing **new safeguards**, you are establishing a new baseline

FOR THE EXAM

…so, compliance with **existing baselines** is not a valid consideration point.

Risk Categories

Category is a group of potential causes of risk.

Damage. Results in physical loss of an asset or the inability to access the asset.

Disclosure. Disclosing critical information regardless of where or how it was disclosed.

Losses. These might be permanent or temporary, including altered data or inaccessible data

Risk Factors

Something that increases risk or susceptibility

Physical damage. Natural disaster, power loss or vandalism.

Malfunctions. Failure of systems, networks, or peripherals.

Attacks. Purposeful acts whether from the inside or outside, such as unauthorized disclosure.

Risk Factors (cont.)

Something that increases risk or susceptibility

Human errors. Usually considered accidental incidents, whereas attacks are purposeful incidents.

Application errors. Failures of the application, including the operating system.

Security Planning

Should include three types of plans

Strategic. Long term, stable plan that should include a risk assessment. (5-yr horizon, annual updates)

Tactical. Midterm plan developed to provide more details on goals of the strategic plan. (usually ~1 year)

Operational. Short-term, highly detailed plan based on the strategic and tactical plans. (monthly, quarterly)

Security Planning

Should include three types of plans

Strategic. **Long term**, stable plan that should include a risk assessment. (5-yr horizon, annual updates)

Tactical. **Midterm** plan developed to provide more details on goals of the strategic plan. (usually ~1 year)

Operational. **Short-term**, highly detailed plan based on the strategic and tactical plans. (monthly, quarterly)

Response to Risk

Risk Acceptance. Do nothing, and you must accept the risk and potential loss if threat occurs.

Risk Mitigation. You do this by implementing a countermeasure and accepting the residual risk.

Risk Assignment. Transfer (assign) risk to 3rd party, like by purchasing insurance against damage.

Risk Avoidance. When costs of mitigating or accepting are higher than benefits of the service

Response to Risk (cont)

Risk Deterrence. Implementing deterrents to would-be violators of security and policy

Risk Rejection. An unacceptable possible response to risk is to *reject* risk or *ignore* risk.

REMEMBER:
Handling risk is not a one-time process!

The primary risk management framework referenced in CISSP is

NIST 800-37

From the CISSP Study Guide

Consider the following RMFs *"for use in the real world"*:

OCTAVE

operationally critical threat, asset, and vulnerability evaluation

FAIR

Factor Analysis of Information Risk

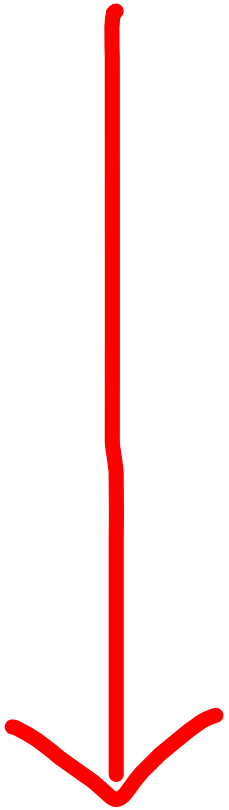
TARA

Threat Agent Risk Assessment

"7 steps of NIST 800-37"

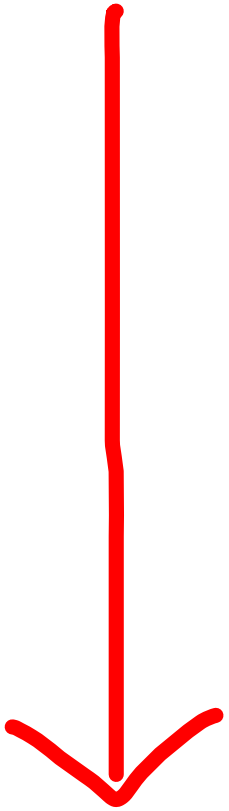
1. **Prepare** to execute the RMF
2. **Categorize** information systems
3. **Select** security controls
4. **Implement** security controls
5. **Assess** the security controls
6. **Authorize** the system
7. **Monitor** security controls

"7 steps of NIST 800-37"



1. **Prepare** to execute the RMF
2. **Categorize** information systems
3. **Select** security controls
4. **Implement** security controls
5. **Assess** the security controls
6. **Authorize** the system
7. **Monitor** security controls

"7 steps of NIST 800-37"



1. **P**repare to execute the RMF
2. **C**ategorize information systems
3. **S**elect security controls
4. **I**mplement security controls
5. **A**ssess the security controls
6. **A**uthorize information system
7. **M**onitor security controls

FOR THE EXAM

You should remember that **not every risk can be mitigated**

FOR THE EXAM

It is **management's job** to decide how that risk is handled

FOR THE EXAM

When multiple priorities present, **human safety** is most important

FOR THE EXAM

When legal issues are involved, **“call an attorney”** is a valid choice

Residual
Inherent
Total
RISK

Residual Risk

The risk that remains even with all conceivable safeguards in place.

Residual Risk

The risk management has chosen to accept rather than mitigate.

Inherent Risk

Newly identified risk not yet addressed with risk management strategies

Inherent Risk

The amount of risk that exists in the absence of controls.

Total Risk

The amount of risk an organization would face if **no safeguards** were implemented.

Residual
Inherent
Total
RISK

Residual AFTER ✓

Inherent BEFORE

✓ Total WITHOUT

FOR THE EXAM

Be able to explain **total risk**, **residual risk**, and **controls gap**

FOR THE EXAM

FORMULAS

To calculate TOTAL RISK, know this formula:

threats * vulnerabilities * asset value = total risk

FOR THE EXAM

FORMULAS

RISK can be defined as follows:

risk = threat * vulnerability

RISK ANALYSIS

Two ways to evaluate risk to assets: qualitative and quantitative

RISK ANALYSIS

Two ways to evaluate risk to assets:
qualitative and **quantitative**

QUANTITATIVE

Assigns a dollar value to evaluate effectiveness of countermeasures

QUANTITATIVE

Assigns a **dollar value** to evaluate effectiveness of countermeasures

OBJECTIVE

Risk Analysis Steps

The six major steps in quantitative risk analysis

1. **Inventory assets** and assign a value *(asset value, or **AV**)*.
2. **Identify threats.** Research each asset and produce a list of all possible threats of each asset. *(and calculate **EF** and **SLE**)*
3. **Perform a threat analysis** to calculate the likelihood of each threat being realized within a single year. *(the **ARO**)*
4. **Estimate the potential loss** by calculating the *annualized loss expectancy (**ALE**)*.
5. **Research countermeasures for each threat,** and then calculate the changes to **ARO** and **ALE** based on an applied countermeasure.
6. **Perform a cost/benefit analysis** of each countermeasure for each threat for each asset.

QUALITATIVE

Uses a scoring system to rank threats and effectiveness of countermeasures

QUALITATIVE

Uses a **scoring system** to rank threats and effectiveness of countermeasures

SUBJECTIVE

DELPHI TECHNIQUE

An **anonymous** feedback-and-response process used to arrive at a consensus.

Should also consider:

Loss potential

What would be lost if the threat agent is successful in exploiting a vulnerability.

Delayed loss

This is the amount of loss that can occur over time.

THREAT AGENTS

are what cause the threats by exploiting vulnerabilities.

THREAT AGENTS

are what cause the threats by **exploiting vulnerabilities.**

Terms and formulas:

Important elements in quantifying potential loss

exposure factor (EF)

single loss expectancy (SLE)

annualized rate of occurrence (ARO)

annualized loss expectancy (ALE)

Safeguard evaluation

Exposure Factor (EF)

Percentage of loss that an organization would experience if a specific asset were violated by a realized risk

Single Loss Expectancy (SLE)

Represents the cost associated with a single realized risk against a specific asset

Single Loss Expectancy (SLE)

SLE = Asset Value (AV) X Exposure Factor (EF)

Single Loss Expectancy (SLE)

AV **EF** **SLE**

$100,000 X .3 (30%) = $30,000

Annualized Rate of Occurrence (ARO)

The expected frequency with which a specific threat or risk will occur within a single year.

Annualized Loss Expectancy (ALE)

The possible yearly cost of all instances of a specific realized threat against a specific asset.

Annualized Loss Expectancy (ALE)

ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO)

ALE Example

Office Building = **$200,000**
Hurricane damage estimate **50%**
Hurricane probability is one every 10 years **10%**

(AV x EF = SLE) $200,000 x .50 = **$100,000**

(SLE x ARO = ALE) $100,000 x .10 = **$10,000**

value of the safeguard (annually)

Safeguard Evaluation

Good security controls mitigate risk, are transparent to users, difficult to bypass, and are cost effective

Safeguard Evaluation

Good security controls **mitigate risk**, are **transparent** to users, **difficult to bypass**, and are **cost effective**

cost effective?

Safeguard Evaluation

ALE before safeguard – ALE after safeguard – annual cost of safeguard = **value of safeguard**

Safeguard Evaluation

value of safeguard = ALE1 – ALE2 - ACS

Controls Gap

The amount of risk reduced by implementing safeguards

Controls Gap

total risk – **controls gap** = residual risk

QUANTITATIVE RISK ANALYSIS

JUST THE FORMULAS!

real-world example!

Available on YouTube

CISSP

EXAM

CRAM

Supply Chain

Today, most services are delivered through a chain of multiple entities

Supply Chain

A secure supply chain includes vendors who are secure, reliable, trustworthy, reputable

Supply Chain Evaluation

When evaluating 3rd parties in the chain, consider:

On-Site Assessment . Visit organization, interview personnel, and observe their operating habits.

Document Exchange and Review . Investigate dataset and doc exchange, review processes

Process/Policy Review . Request copies of their security policies, processes, or procedures.

Third-party Audit. Having an independent auditor provide an unbiased review of an entity's security infrastructure

Threat Modeling

Can be ***proactive*** or ***reactive***, but in either case, goal is to eliminate or reduce threats

3 approaches to threat modeling

Common approaches to threat modeling:

Focused on Assets. Uses **asset valuation** results to identify threats to the valuable assets.

Focused on Attackers. Identify potential attackers and identify threats based on the **attacker's goals**

Focused on Software. Considers **potential threats** against the software the org develops.

STRIDE

developed by Microsoft

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

PASTA

Stage I: Definition of Objectives

Stage II: Definition of Technical Scope

Stage III: App Decomposition & Analysis

Stage IV: Threat Analysis

Stage V: Weakness & Vulnerability Analysis

Stage VI: Attack Modeling & Simulation

Stage VII: Risk Analysis & Management

focuses on developing countermeasures based on asset value

DOMAIN 1: THREAT MODELING

VAST

based on Agile PM principles

Visual

Agile

Simple

Threat

GOAL: Scalable integration of threat management into an Agile programming environment

DREAD

based on answer to 5 questions

Damage potential

Reproducibility

Exploitability

Affected users

Discoverability

TRIKE

focused on "acceptable risk"

An open-source threat modeling process that implements a requirements model.

Ensures the assigned level of risk for each asset is "acceptable" to stakeholders.

COBIT

security control framework

IT management and governance framework

Principle 1: Meeting Stakeholder Needs

Principle 2: Covering the Enterprise End-to-End

Principle 3: Applying a Single, Integrated Framework

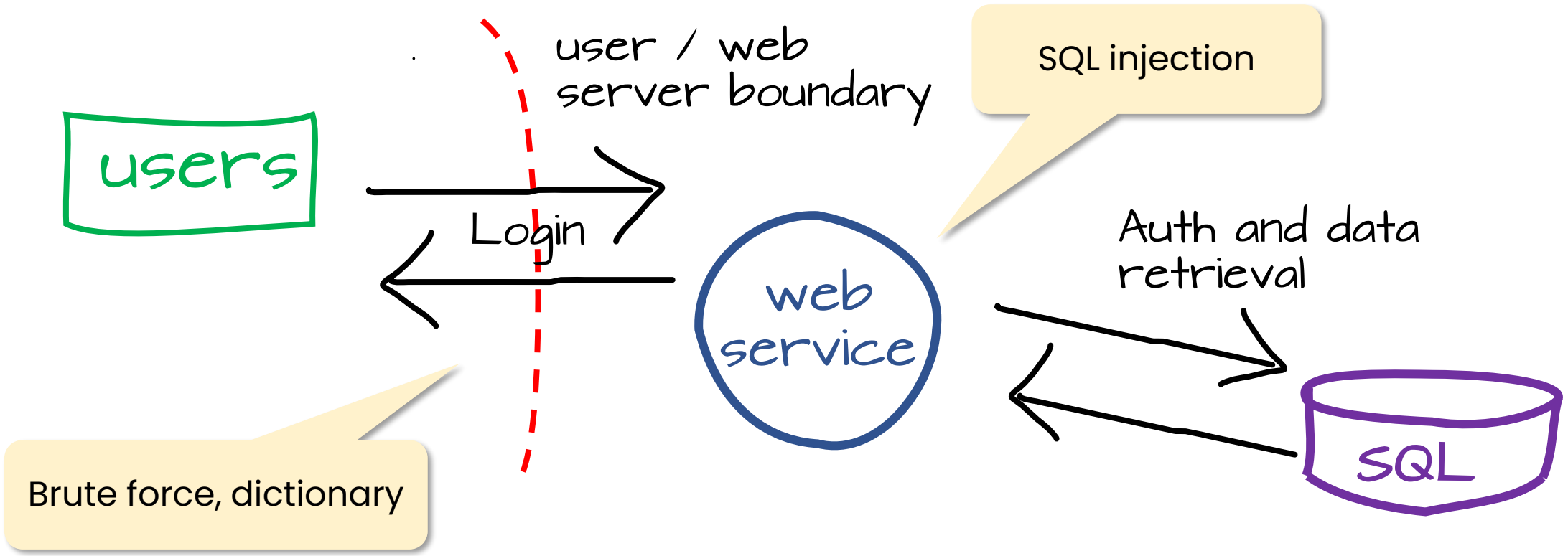
Principle 4: Enabling a Holistic Approach

Principle 5: Separating Governance from Management

little coverage and no depth on CISSP !

Diagramming Potential Attacks

Determining potential attack concepts is often achieved through diagramming



DIAGRAMMING POTENTIAL ATTACKS

Reduction Analysis

Trust Boundaries. Any location where the level of trust or security changes

Data Flow Paths. The movement of data between locations

Input Points. Locations where external input is received

Privileged Operations. Any activity that requires greater privileges than of a standard user account

Details about Security Stance and Approach. declaration of security policy, security foundations, and security assumptions.

Prioritization and Response

Then threats are ranked or rated using DREAD, high/medium/low rating, etc.

Security Controls

Security measures for countering and minimizing loss or unavailability of services or apps due to vulnerabilities

Security Controls

The terms **safeguards** and **countermeasure** may seem to be used interchangeably

Security Controls

safeguards are **proactive**
countermeasure are **reactive**

Control Categories

There are three categories of security controls:

Technical. aka “logical”, involves the hardware or software mechanisms used to manage access.

Administrative. Policies and procedures defined by org’s security policy, other regulations and requirements

Physical. Are items you can physically touch.

Control Types

Deterrent. Deployed to discourage violation of security policies.

Preventative. Deployed to thwart or stop unwanted or unauthorized activity from occurring.

Detective. Deployed to discover or detect unwanted or unauthorized activity.

Compensating. Provides options to other existing controls to aid in enforcement of security policies.

Control Types

Deterrent. Deployed to **discourage violation** of security policies.

Preventative. Deployed to thwart or **stop unwanted or unauthorized activity** from occurring.

Detective. Deployed to **discover or detect** unwanted or unauthorized activity.

Compensating. Provides **options to other existing controls** to aid in enforcement of security policies.

Control Types (cont)

Corrective. modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred.

Recovery. an extension of corrective controls but have more advanced or complex abilities.

Directive. direct, confine, or control the actions of subjects to force or encourage compliance with security policies

Control Types (cont)

Corrective. modifies the environment to **return systems to normal** after an unwanted or unauthorized activity has occurred.

Recovery. an **extension of corrective controls** but have more advanced or complex abilities.

Directive. direct, confine, or **control the actions of subjects** to force or encourage compliance with security policies

legal and regulatory issues that pertain to information security in a **global context**

- Cyber crimes and data breaches
- Trans-border data flow
- Licensing and intellectual property requirements
- Privacy
- Import/export controls

Types of Law

Criminal Law. contains prohibitions against acts such as murder, assault, robbery, and arson.

Civil Law. include contract disputes, real estate transactions, employment, estate, and probate.

Administrative Law. Government agencies have some leeway to enact administrative law.

CISSP exam focuses on security-related generalities of law, regulations, investigations, and compliance

Laws

Computer Fraud and Abuse Act (CFAA) . The first major piece of US cybercrime-specific legislation

Federal Sentencing Guidelines. provided punishment guidelines to help federal judges interpret computer crime laws.

Federal Information Security Management Act (FISMA). Required a formal infosec operations for federal gov't

Copyright and the Digital Millennium Copyright Act. Covers literary, musical, and dramatic works.

IP and Licensing

Trademarks. covers words, slogans, and logos used to identify a company and its products or services.

Patents. Patents protect the intellectual property rights of inventors.

Trade Secrets. intellectual property that is absolutely critical to their business and must not be disclosed.

Licensing. 4 types you should know are contractual, shrink-wrap, click-through, and cloud services.

Encryption and Privacy

Computer Export Controls. US companies can't export to Cuba, Iran, North Korea, Sudan, and Syria.

Encryption Export Controls. Dept of Commerce details limitations on export of encryption products outside the US..

Privacy (US). The basis for privacy rights is in the Fourth Amendment to the U.S. Constitution.

Privacy (EU). General Data Protection Regulation (GDPR) is not a US law, but very likely to be mentioned!

Applies to any company with customers in the EU!

Other US privacy laws

HIPAA (Health Insurance Portability and Accountability Act)

HITECH (Health Information Technology for Economic and Clinical Health)

Gramm-Leach-Bliley Act (financial institutions)

Children's Online Privacy Protection Act (**COPPA**) ✓

Electronic Communications Privacy Act (**ECPA**) ✓

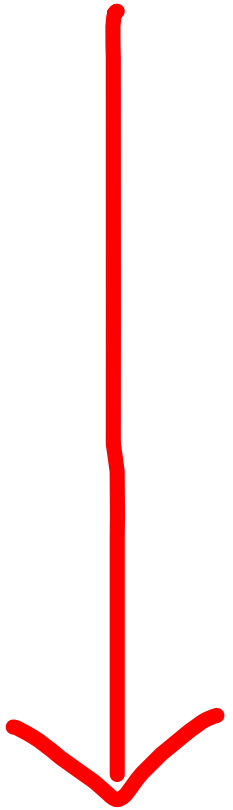
Communications Assistance for Law Enforcement Act (**CALEA**) ✓

Business continuity planning issues that pertain to information security in

1. Strategy development
2. Provisions and processes
3. Plan approval
4. Plan implementation
5. Training and education

Business continuity planning issues that pertain to information security in

1. Strategy **development**
2. Provisions and **processes**
3. Plan **approval**
4. Plan **implementation**
5. Training and **education**



DOMAIN 1: USER EDUCATION

Establish and maintain a **security awareness, education, and training** program

- Methods and techniques to present awareness and training
- Periodic content reviews
- Program effectiveness evaluation