A Strategic Guide For Our Yearly Plan Subscribers

By joining the full Security Professional Plan, you've unlocked everything. Here's what that actually means for your success for the CISSP exam:

Total Video Hours Available

- **CISSP Course**: 61 hours of detailed, domain-by-domain video training
- **The SONIC Project (CC Exam Course)**: 13 hours of foundational cybersecurity content
- **CCSP Course**: 15 hours of cloud-focused advanced learning
  → **That's 89 hours of video training total**

Total Practice Questions

- **CISSP Practice Questions**: 900 ultra-difficult, scenario-based questions
- **CC Exam Course Questions**: 250 foundational questions
- **CCSP Course Questions**: 300 cloud and compliance-driven questions
  → **That's 1,450 total questions to test your knowledge**

Additional Learning Tools Included:

- 1,500 Flashcards
- Final Push CISSP Review E-Book
- Study Notes and Theory Telegram Group (lifetime access)
- CISSP Podcast – Orbital Strike: Dozens of mindset and domain-linked episodes

This is more than a course—it's a **complete, multi-layered CISSP learning system**. Each resource is designed to reinforce the others. Each question, video, and page builds toward the one thing that matters:

Putting "CISSP" after your name.

How to Use All Resources Across CISSP Domains

DOMAIN 1: Security and Risk Management

Understanding governance and ethics is the launching point for CISSP. But the real strength of this domain comes from how it applies everywhere else. For example, a strong risk management framework impacts how you evaluate third-party contracts (Domain 7), prioritize controls (Domain 2), or even plan secure system designs (Domain 3). The idea of due care and due diligence here is the philosophical anchor that guides every other decision you make in cybersecurity. Start here. Build your CISSP mindset and risk management foundation.

Study Notes and Theory stands out by layering risk and ethics concepts from beginner-level CC lessons to expert-level CISSP analysis. You don't just memorize, you evolve. The Final Push book adds real-world framing, while the podcast turns theory into practical wisdom.

CC Course:
1.1 Security Concepts (Confidentiality, Integrity, Availability),
1.2 Risk Management,
1.4 ISC2 Code of Ethics
These videos give you a beginner-friendly foundation of what information security is, why it matters, and how it connects to the broader landscape of the CISSP. Watching these first transforms vague ideas into concrete terms, so when you hit more advanced material, it feels familiar—not foreign.

CISSP Course:
CIA Triad, Risk Management Part 1 & 2, Code of Ethics, Recovery Strategy, BCP/DRP Phases
These videos elevate your thinking from a technical role to a risk-driven, policy-aware mindset. You begin to see how decisions impact business continuity, not just systems—an essential leap for CISSP mastery.

Books:

- **Sybex:** Chapter 1
- **Shon Harris:** Domain 1
- **Think Like a Manager:** *Questions 2, 5, 6, 11, 13, 15, 16*
  These questions guide you through foundational decisions around risk, policy enforcement, business continuity, third-party assessments, and due diligence. They teach you to think like a risk owner, not just a risk analyst.

Final Push:
Chapter 2
This chapter sharpens your exam instincts. It gives you practice identifying "the step within the step"—the real trick behind most CISSP questions—while reinforcing what you just learned in video and reading form.

Podcast:
"The CISSP Mental Game,"
"How I Know You Will Become a CISSP"
These episodes put it all together. You internalize what it feels like to be a CISSP—not just what you need to memorize. The mindset shift here is what keeps you from burning out or second-guessing your progress.

CCSP Course:
Domain 1 – Cloud Concepts, Architecture and Design
This domain shows how governance shifts when you're no longer in full control of the infrastructure. You'll see how cloud-specific roles and shared responsibility models affect every decision—from policy to risk assessment. Use this as your bridge between on-premise control and cloud delegation.

DOMAIN 2: Asset Security

Asset Security is where theory becomes tactical. It's not just about labeling data—it's about knowing what you're protecting, why it matters, and how bad it would be if it got out. This domain teaches you how to classify, retain, and destroy information according to its value and sensitivity. But more importantly, it helps you think like a security leader who doesn't just protect all data equally—you protect what matters most, where it matters most.

This domain reaches across every other: it influences access decisions (Domain 5), encryption strategies (Domain 3), and even how you handle logs and privacy (Domain 7). Study Notes and Theory brings these concepts to life by combining breach simulations, control comparisons, and real-world case studies. The Final Push drills your ability to spot subtle distinctions—like when to use encryption vs. access control—while the podcast episodes shift your mindset from checkbox security to calculated protection based on business impact.

CC Course:
Data Classification, Data Lifecycle, Encryption Basics
These foundational lessons give you the vocabulary and structure around protecting data at every stage—from creation to deletion. This primes your brain to spot what's sensitive, why it matters, and where it lives—a huge advantage before diving into more advanced CISSP topics.

CISSP Course:
Classification Labels, Administrative/Technical/Physical Controls, Just-In-Time Access, Breach Attack Simulation
Here's where theory meets design. You begin to grasp not just what controls exist, but why you'd apply them to different asset classes. The breach simulations take abstract policies and make them feel real—and memorable.

Books:

- **Sybex:** Chapter 2
- **Shon Harris:** Domain 2
- **Think Like a Manager:** *Questions 1, 3, 21*
  These questions walk you through media sanitization, data labeling, ownership roles, and chain-of-custody scenarios. They help you recognize where human error and policy gaps intersect—and what you'd do about it as a manager.

Final Push:
Chapter 3
This chapter helps you compare control types quickly, recognize subtle distinctions in test questions, and identify asset vulnerabilities using real-world logic.

Podcast:
"Study Like an Investor, Win Like a CISO"
This episode reinforces that securing data isn't about blanket rules—it's about calculated risk management aligned to business impact. It reinforces how to think, not just what to memorize.

CCSP Course:
Domain 2 – Cloud Data Security
The CCSP course here shows how data classification, storage, retention, and destruction change in cloud environments. You'll see how asset protection strategies apply when the data is on someone else's infrastructure—and what controls still remain in your hands.

DOMAIN 3: Security Engineering

This domain doesn't live in a vacuum—it's the skeleton that supports Domain 4's secure network flows, Domain 8's secure coding practices, and Domain 6's system testing. Think about how implementing a secure cryptographic module (Domain 3) must also be tested under Domain 6. Or how Bell-LaPadula access restrictions support the classifications established in Domain 2. We highlight these technical overlaps so you never study in isolation. We combine deep-dive cryptography lessons with vivid analogies and real attacks. Using CCSP here is a unique Study Notes and Theory advantage—most platforms don't tie cloud roles back to CISSP engineering principles.

Study Notes and Theory walks you through classic security models with storytelling and step-by-step animations, so concepts like Clark-Wilson and Biba feel less like academic trivia and more like system design tools. The Final Push brings it together with real-life decision breakdowns and cryptographic logic trees.

CC Course:
3.1 & 3.2 Physical & Logical Access Control
These videos explain the most essential access control models in plain terms. They're not just theory—they give you mental hooks that make everything in cryptography, firewalls, and application controls easier to grasp later.

CISSP Course:
Bell-LaPadula, Biba, Clark-Wilson, Public Key Infrastructure, Cryptography Attacks, SCADA
This is where you stop reading about controls and start designing with them. These models train you to understand both the philosophy and the practicality behind confidentiality, integrity, and availability.

Books:

- **Sybex:** Chapters 3–4
- **Shon Harris:** Domain 3
- **Think Like a Manager:** *Questions 7, 9, 10, 12*
  These questions help you distinguish integrity models, digital signatures, and critical design decisions involving control implementation. You'll think through how to protect systems not just from attackers—but from bad architecture.

Final Push:
Chapter 4
This chapter turns cryptography into a functional concept. It walks you through the *why* of encryption choices—not just the definitions—so you can pick the best method on the exam and in the real world.

Podcast:
"The Concept Connection," "SAML Architecture and Risks"
These episodes help you mentally organize complex ideas. You'll stop seeing engineering topics as separate and start seeing how they converge across domains like identity, data classification, and access.

CCSP Course:
Domains 1 & 3 – Cloud Architecture and Infrastructure Security
This is where you start seeing cryptographic responsibilities shift in cloud environments. It shows how what you learned in traditional architecture now applies across distributed systems, shared responsibility models, and virtualization layers.

DOMAIN 4: Communication and Network Security

You can't build secure networks unless you understand what you're protecting and who should access it. VPNs, TLS, VLANs—these are not just technologies but execution tools for the policy decisions in Domains 1 and 2. For example, when an organization chooses to isolate sensitive data, VLAN segmentation (Domain 4) and encryption (Domain 3) ensure those intentions are carried out. We connect these dots in every lesson. We teach the OSI model through active comparison, storytelling, and actual configuration breakdowns. Our network content ties together CISSP, CC, and podcast insights in a way few courses attempt.

Study Notes and Theory transforms network security from protocol memorization into high-level decision-making. The Final Push tells you exactly what to care about for the exam, and *Think Like a Manager* shows how even a basic network design question is really a test of layered thinking, business requirements, and risk tolerance.

CC Course:
OSI Model Parts 1–6, Basic Network Design, TCP vs UDP
These CC videos demystify how networks move data. They help you visualize the 'stack' and understand what each layer protects—so when you get to firewalls, ports, or VPNs in CISSP, you already know how the pieces work together.

CISSP Course:
TCP Handshake, OSI Model, Firewall Architectures, VLANs, TLS, IPSec
This is the application layer of your network knowledge—literally and figuratively. These lessons transform diagrams into decisions, helping you understand not just how, but why networks are secured in specific ways.

Books:

- **Sybex:** Chapter 4
- **Shon Harris:** Domain 4
- **Think Like a Manager:** *Questions 8, 14, 24*
  These questions walk you through firewall architecture, DMZ design, multi-layer protections, and OSI-based attack identification. They force you to step out of “how does it work” and into “why was this the best choice.”

Final Push:
Chapter 5
This chapter helps you cut through the noise. It focuses on the most testable network security details while reinforcing them with strategic reasoning, not rote memorization.

Podcast:
"How Does the OSI Model Actually Work?"
This episode breaks down conceptual barriers. You’ll finally see the OSI model not as an abstract diagram—but as a tool to analyze and predict real-world security behavior.

CCSP Course:
Domain 3 – Cloud Infrastructure, Virtual Networking, VPNs
The CCSP videos show you how traditional network controls like firewalls, segmentation, and secure channels evolve in a multi-tenant, virtualized cloud environment. You’ll get a modern take on VLANs, zero trust networking, and shared network access boundaries.

DOMAIN 5: Identity and Access Management

IAM is how all other domains are enforced. Think of it as the mechanism through which Domain 2's data classification or Domain 7's operational workflows come alive. A file labeled "Highly Confidential" is only as secure as the SAML token that validates the user trying to access it. Without proper identity, even the best security controls fail—and that's a message we hammer into every scenario-based lesson. Study Notes and Theory gives you layered identity knowledge, from simple definitions to the nuance of federated identity design. You won't just know what SAML is—you'll know when it breaks, and why.

CC Course:
Logical Access Control, RBAC, MAC, DAC
These lessons give you the language and logic of identity management. You'll understand the difference between access types in a way that sticks, preparing you for complex federated identity concepts later in CISSP and CCSP.

CISSP Course:
Federated Identity, SAML, OAuth, OpenID, SPML
These videos take access management to the enterprise level. You'll learn how identity travels across domains, vendors, and protocols—and how mistakes in this layer lead to breaches.

Books:

- **Sybex:** Chapter 5
- **Shon Harris:** Domain 5
- **Think Like a Manager:** *Questions 17, 22*
  These questions help you think through access provisioning, single sign-on risks, and identity decisions with business consequences. They're less about the acronyms and more about *why* you'd trust or reject a federated provider.

Final Push:
Chapter 6
This chapter helps you confidently answer identity and access questions by breaking down the logic of what the test is really asking—not just what the terms mean.

Podcast:
"SAML Architecture and Risks"
This episode explores not just what SAML does—but what happens when it fails. The lessons carry over directly into decision-making scenarios you'll see on the exam.

CCSP Course:
Domain 4 – Cloud Identity Models, Federation, SSO
These CCSP lessons teach you how identity transforms in cloud. You'll learn how traditional IAM maps to service models, and how access control decisions span organizations in multi-cloud and hybrid setups.

DOMAIN 6: Security Assessment and Testing

Assessment isn't just a checkpoint—it's a loop that touches everything. We test if access controls are working (Domain 5), if the cryptographic protocols are properly implemented (Domain 3), or if IR plans (Domain 7) are effective. This domain teaches you to ask, "Are we secure?"—but also, "How do we know?" Study Notes and Theory excels at making these feedback loops concrete and repeatable. We blend compliance, pen testing, and assurance with teaching strategies that mimic real-life audit and control environments.

CC Course:
5.1 Logging & Monitoring, 5.2 System Hardening
These lessons lay the groundwork for assessing whether your defenses are working. You learn the importance of baselines and visibility—concepts that carry into CISSP's assurance framework.

CISSP Course:
Pen Test vs Red Team, SOC Reports, Reverse Practice Questions, Assurance
These videos show you how to evaluate controls in action. You'll begin thinking like an auditor, knowing where to look for weaknesses even if everything appears compliant.

Books:

- **Sybex:** Chapter 6
- **Think Like a Manager:** *Questions 4, 19*
  These questions walk through ethical hacking, pen testing boundaries, and how to report findings without overstepping scope. They reinforce the balance between technical exploration and business-level justification.

Final Push:
Chapter 7
This chapter walks you through the art of verification—identifying what matters in a test question when terms like "audit," "assess," and "review" are all tempting.

Podcast:
"The $500 Million Data Breach Case"
This episode connects failures in assessment to real-world consequences, helping you remember why this domain matters beyond the test.

CCSP Course:
Domain 6 – Audit and Compliance
These videos demonstrate how testing and assessments are performed in shared responsibility environments, where you can’t just test a system—you have to coordinate it.

DOMAIN 7: Security Operations

This is where all planning and protection come together. Operations is what happens when the world doesn't care about your policies or design. You need to execute fast, using tools from Domain 6 (testing), access logic from Domain 5 (least privilege), and restoration plans from Domain 1 (BCP/DRP). Our Malware IR series shows you exactly how to pivot between domains in a real emergency. Our incident response breakdowns come with real-world rhythm—you feel the urgency, you think through the containment.

CC Course:
Security Awareness, Incident Response Lifecycle, Backup Concepts
These videos help you understand response planning from the ground up. They make operational security concepts stick by showing how everyday roles support major incident plans.

CISSP Course:
Malware IR Series, Industrial Controls, Due Care, IDS/ICS Practice Questions
These videos simulate pressure. They train you to respond quickly, align your response to policy, and understand where operational roles intersect with strategy.

Books:

- **Shon Harris:** Domain 7
- **Think Like a Manager:** *Questions 18, 23*
  These questions bring you into post-breach decision making, privilege misuse, and policy violations. They show how operations is where risk management becomes reality.

Final Push:
Chapter 8
This chapter helps reinforce IR process thinking—what comes first, what must be escalated, and how to stay inside policy under pressure.

Podcast:

"CISSPs on Paper vs. CISSPs in Action"

This episode highlights why operations separates certified professionals from capable ones. You'll reflect on what it means to actually *handle* security, not just study it.

CCSP Course:

Domain 5 – Cloud Operations, Monitoring, and Response

These lessons show how incident response, forensics, and operational workflows scale in the cloud. You'll learn why visibility and automation are just as important as procedures.

DOMAIN 8: Software Development Security

Every domain feeds into secure development. From governance requirements (Domain 1) to encryption protocols (Domain 3) to identity integration (Domain 5), software security is the ultimate test of holistic CISSP thinking. We use real-world examples to show how failing in one domain—say, logging (Domain 6) or access control (Domain 5)—can compromise everything in your codebase.

Study Notes and Theory ensures you see the system, not just the syntax. We teach SDLC with layered context—starting with clean diagrams and ending with breach case studies and agile pipelines. Then we take it further with CCSP's secure code and compliance models.

CC Course:
SDLC Overview, Secure Coding Principles
These videos lay the foundation for secure software thinking. They teach you the phases of development and the risks introduced at each step before you even reach CISSP content.

CISSP Course:
CI/CD Correlation Series, SDLC Phases, Application Security Considerations, SQL Injection
These videos connect development life cycles to business risk. You learn how security fits inside Agile, DevOps, and other fast-paced release cycles—critical knowledge for modern CISSPs.

Books:

- **Sybex:** Chapter 8
- **Think Like a Manager:** *Questions 20, 25*
  These questions take you into real-world dev decisions: rushed releases, broken SDLC pipelines, missing controls in third-party code. They bring life to a domain often taught in dry checklists.

Final Push:
Chapter 9
This chapter breaks SDLC wide open. You'll know which phase introduces the most risk, which should have started earlier, and how secure development is really just cross-domain awareness in motion.

Podcast:
"The Software Development Lifecycle – Real-Life Examples"
This episode makes SDLC memorable by showing it in action: real mistakes, real timelines, and real impact.

CCSP Course:
Domain 4 – Cloud Software Development and Secure SDLC
You'll see how CI/CD pipelines work in distributed environments, and how dev teams must now think about containers, APIs, and compliance from Day One.

Reinforcement Strategy

- Use the **Final Push E-Book** after every domain to summarize and test your understanding.
- Use the **Podcast** to reflect and reinforce during passive time (commute, gym, walk).
- Rotate in **CC course videos** early in the process to simplify foundational material.
- Use **CCSP course videos** mid-to-late to help with cloud-heavy domains like 3, 4, 5, and 8.
- Attempt **15–20 of the 900 CISSP questions** per domain and review answers *immediately*.
- Join the **Telegram group** to discuss the domain you're working on weekly.

Study Notes and Theory isn't just a course—it's an integrated CISSP learning system that leaves no gaps. Every question, video, flashcard, and case study connects back to the same outcome: passing *your* CISSP exam.

Listen, "**good things come to those who wait**" is a lie told to the slow and the hesitant. Waiting around achieves absolutely nothing—*especially* in cybersecurity. Life problems pop up? You need to smash them instantly. Opportunity rewards those who act decisively. In cybersecurity, especially in today's rapidly shifting environment, hesitation isn't strategy—it's a death sentence for your career ambitions. Your CISSP certification won't come knocking on your door; it demands immediate, deliberate action. I curated this complete system as your express ticket to success - all within 1 year. You won't find this level of value anywhere else online. With a full market price of $1,108.86, our Security Professional Plan is available now for $599. If you find a better price for the value, feel free to tell me about it!

If you use these resources the way they're meant to be used, you won't have a choice *but* to pass. And once you do—who knows? You might even find yourself going for your CCSP next… or before your CISSP ever clears the exam system.

All the best future CISSP,
Luke Ahmed
https://www.studynotesandtheory.com/