Data Security Essentials (DS0-001)

CompTIA DS0-001 Data Security. Threat identification, security controls, and compliance for IT pros.

IT Certifications Instructor: Brian Taylor • 5 sections • 45 lessons • 15.25h total

View this course online Browse all courses

About this course

This course provides a practical guide to the core concepts covered in the CompTIA Data Security Essentials (DS0-001) exam. We focus on real application, moving beyond theory to show how modern data protection principles are implemented in business environments. You will learn how to identify threats, apply security controls, and understand the compliance landscape that governs data privacy.

We will walk you through each key domain with step-by-step guides, problem-solving sessions, and real case study analysis. You will get hands-on with downloadable templates for risk assessments and policy creation.

Course curriculum

Foundations of Data Security

- Understanding the Data Security Landscape (12m)
  We'll explore why data security is critical today, covering key concepts like the CIA Triad and setting the stage for the rest of the course.
- Identifying and Classifying Your Data Assets (18m)
  Learn a step-by-step guide to classifying data (PII, PHI, etc.) so you can apply the right level of protection from the start.
- Core Security Principles: Defense in Depth (15m)
  A practical look at the layered security approach, with real-world examples of how each layer protects your critical assets.
- Threat Modeling Basics for Your Organization (22m)
  A problem-solving session on identifying potential threats and vulnerabilities specific to your business environment.
- Introduction to Security Policies and Procedures (14m)
  We'll show you how to read and understand the foundational documents that govern security in any organization.
- The Role of Compliance in Data Security (16m)
  An overview of major regulations like GDPR and HIPAA and how they directly impact your daily security tasks.
- Building a Security-First Mindset (9m)
  Learn how to develop the habits and awareness that make you a strong first line of defense against social engineering and other attacks.

Core Security Controls and Operations

- Implementing Strong Access Control Measures (25m)
  A deep dive into Authentication, Authorization, and Accounting (AAA), with a downloadable template for reviewing user permissions.
- Securing Data at Rest: Encryption Fundamentals (28m)
  Understand how encryption works for stored data, including a practical case study on choosing the right encryption standards.
- Protecting Data in Transit: Network Security Basics (23m)
  We'll break down how protocols like TLS and VPNs protect data as it moves across networks, with simple, clear examples.
- Network Hardening: Firewalls and Intrusion Detection (32m)
  A step-by-step guide to basic firewall rules and an introduction to IDS/IPS systems to monitor for suspicious activity.
- Endpoint Security: Protecting Devices and Data (20m)
  Learn the essential controls for securing laptops, servers, and mobile devices, including anti-malware and device management.

- The Security Incident and Event Management (SIEM) Process (26m)
  A practical look at how SIEM tools help you collect and analyze log data to spot security events in real time.
- Vulnerability Management: Scanning and Prioritization (19m)
  We'll show you how to run a vulnerability scan and, more importantly, how to decide which patches to apply first.
- Data Sanitization: Secure Disposal of Media (11m)
  A short but crucial lesson on the proper methods for destroying data on old hard drives and devices.
- Secure Software Development Lifecycle (SDLC) (21m)
  An overview of how to build security into software from the beginning, preventing vulnerabilities before they happen.

Deep Dive: Identity, Authentication, and Cryptography

- Modern Authentication: MFA and Beyond (24m)
  Explore Multi-Factor Authentication (MFA) and passwordless solutions with a real case study on preventing account takeovers.
- Public Key Infrastructure (PKI) Explained Simply (30m)
  A problem-solving session that demystifies certificates, keys, and how they create trust online.
- Cryptography: Symmetric vs. Asymmetric Algorithms (27m)
  We'll compare different encryption types and discuss when to use each for maximum security and performance.
- Implementing Key Management Best Practices (18m)
  Learn the critical steps for securely generating, storing, and rotating encryption keys using a downloadable checklist.
- Digital Signatures and Data Integrity (13m)
  Understand how digital signatures prove that data hasn't been tampered with, a key concept for compliance.
- Identity Federation: SSO and Directory Services (29m)
  A practical guide to how Single Sign-On (SSO) works and how it simplifies access management across multiple systems.
- Role-Based Access Control (RBAC) in Practice (17m)
  We'll show you how to design and implement RBAC to ensure users only have access to the data they absolutely need.

Advanced Application: Monitoring and Incident Response

- Building an Effective Incident Response Plan (31m)
  A step-by-step guide to creating a clear, actionable plan for what to do when a security breach occurs.
- The 6 Phases of Incident Response: Preparation (15m)
  We'll focus on the preparation phase, showing you how to set up your team and tools for success before an incident.

- Detection and Analysis: Spotting the Threat (22m)
  A problem-solving session on using logs and alerts to determine if you're facing a real security threat or a false alarm.
- Containment, Eradication, and Recovery (26m)
  Learn the critical actions to take to stop an attack, remove the threat, and restore normal operations safely.
- Post-Incident Activity: Lessons Learned (12m)
  Discover how to conduct a post-mortem analysis to strengthen your defenses and prevent future attacks.
- Forensics Fundamentals for Data Security (20m)
  An introduction to the basics of digital forensics and how to preserve evidence for legal or internal review.
- Disaster Recovery and Business Continuity Planning (28m)
  A real case study on how companies recover from major data loss events and maintain operations.
- Configuring and Managing Security Alerts (19m)
  We'll show you how to tune your SIEM and other tools to reduce alert fatigue and focus on what matters.
- Data Backup Strategies for Resilience (16m)
  A practical guide to the 3-2-1 backup rule and testing your backups to ensure they actually work when you need them.
- Chain of Custody and Legal Considerations (10m)
  A short lesson on the importance of maintaining a clear chain of custody for evidence during an investigation.

Implementation, Governance, and Next Steps

- Developing a Data Governance Framework (25m)
  A problem-solving session on creating policies for data ownership, quality, and lifecycle management.
- Risk Management: Assessment and Mitigation (33m)
  We'll use a downloadable risk assessment template to walk you through identifying, analyzing, and treating security risks.
- Third-Party Risk Management: Vendor Security (21m)
  Learn how to evaluate the security posture of your vendors and partners to protect your supply chain.
- Auditing and Logging for Accountability (18m)
  A practical guide to setting up effective logging to track who did what, and when, across your systems.
- Data Privacy: From Policy to Practice (23m)
  We'll show you how to translate high-level privacy policies into concrete technical and administrative controls.
- Security Awareness Training: A Practical Guide (14m)
  Learn how to create and deliver engaging training that actually changes employee behavior.
- Change Management in a Secure Environment (16m)
  Understand how to implement changes to systems and processes without introducing new vulnerabilities.

- Preparing for the DS0-001 Exam: Key Topics (27m)
  A focused review of the most critical DS0-001 domains and a downloadable study plan to guide your final preparation.
- Practice Questions and Scenario Analysis (35m)
  We'll work through sample questions and scenarios together, explaining the logic behind the correct answers.
- Career Paths in Data Security (11m)
  An honest conversation about where a DS0-001 certification can take you and what to focus on for your next role.
- Staying Current: The Evolving Threat Landscape (13m)
  Learn reliable sources and communities to follow so your data security knowledge stays sharp and up-to-date.
- Course Wrap-Up and Your Action Plan (8m)
  A final summary of the key takeaways and a clear set of next steps to continue your data security journey.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

Visit the blog All courses This course