CS-002 · Foundations

The CIA Triad

Confidentiality, integrity, and availability, the three goals every security control serves.

Executive Summary

The CIA triad describes the three fundamental goals of information security: keeping data confidential, preserving its integrity, and ensuring its availability. Nearly every security control exists to protect one or more of these three properties. It is the mental model professionals use to reason about what they are actually trying to defend.

What It Is

The CIA triad is a model that breaks information security into three objectives. Confidentiality means that only authorized people and systems can see the data. Integrity means the data is accurate, complete, and has not been altered without authorization, whether by an attacker or by accident. Availability means the data and the systems that serve it are accessible to authorized users when they are needed. Every meaningful security decision can be traced back to one or more of these goals, which is why the triad appears in almost every security framework and certification.

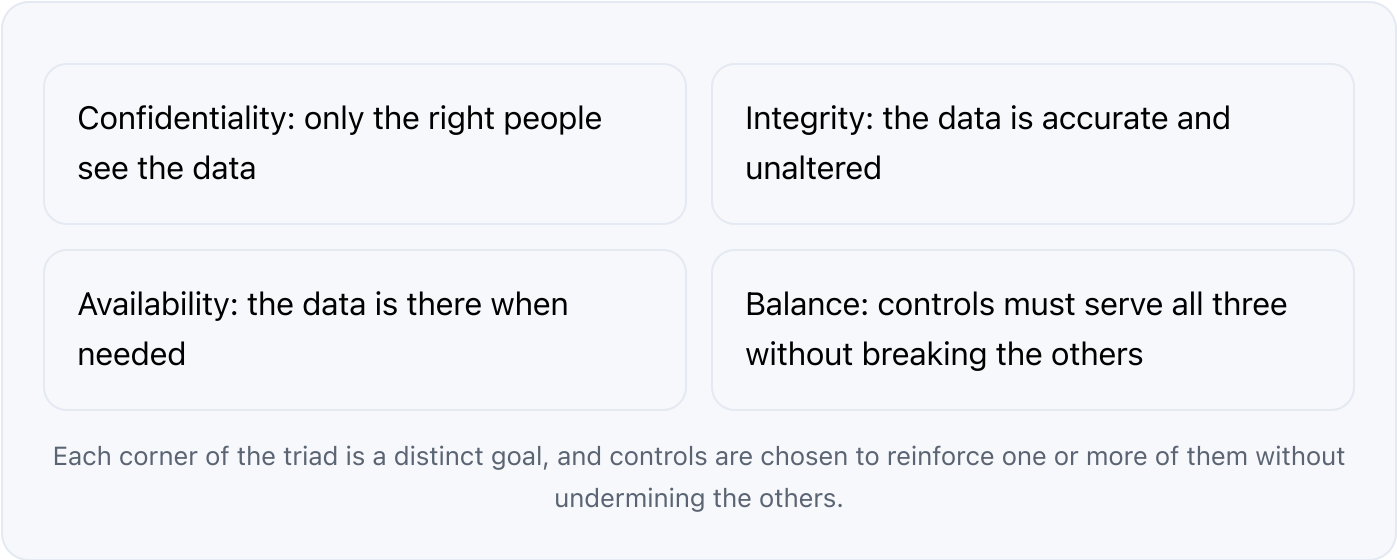
Why It Matters

The triad gives teams a shared language for trade-offs. Locking a system down tightly can protect confidentiality but hurt availability if legitimate users cannot get in. Rushing to restore availability after an outage can undermine integrity if it means recovering from unverified data. Understanding which property a control protects, and which it might weaken, lets professionals make deliberate choices instead of accidental ones. For anyone in a security, risk, audit, or governance role, being able to map a threat or a control to the triad is a baseline expectation.

How It Works

In practice, teams choose controls that reinforce each property. Confidentiality is supported by access control, encryption, and data classification. Integrity is supported by hashing, digital signatures, version control, and change management. Availability is supported by redundancy, backups, capacity planning, and resilient architecture. A single control often serves more than one goal at once, and a single incident often threatens more than one. Ransomware, for example, attacks availability by locking files, and increasingly attacks confidentiality by stealing them first. The triad is a checklist for reasoning, not a set of products.

Architecture Diagram



Each corner of the triad is a distinct goal, and controls are chosen to reinforce one or more of them without undermining the others.

Visual Workflow

Review the balance again as the system and its data change.

Common Attacks

- Data theft and eavesdropping that break confidentiality
- Tampering with records, files, or transactions that breaks integrity
- Denial of service and ransomware that break availability
- Man in the middle attacks that can break confidentiality and integrity at once
- Insider misuse that quietly undermines any of the three goals

Common Mistakes

- Focusing only on confidentiality and forgetting integrity and availability
- Adding controls without noticing they harm availability for legitimate users
- Treating backups as an availability control while never checking their integrity
- Assuming encryption alone protects data that is also at risk of tampering
- Failing to classify data, so every asset is protected the same generic way

Best Practices

- Classify data so protection matches its sensitivity and importance
- Use encryption in transit and at rest to protect confidentiality
- Use hashing, signatures, and change control to protect integrity
- Build redundancy and tested backups to protect availability
- Document which goal each major control serves
- Review trade-offs whenever a control noticeably slows or blocks users

Quick Checklist

- [ ] Data classification scheme defined and applied to key assets
- [ ] Encryption in transit and at rest for sensitive data

- [x] Integrity checks (hashes or signatures) on critical files or records
- [x] Redundancy or failover for systems that must stay available
- [x] Backups tested with a verified, clean restore
- [x] Access reviews confirming only authorized users can reach the data

Recommended Tools

Encryption tools (TLS, disk and file encryption)
Protect confidentiality of data in transit and at rest

Hashing and file integrity monitoring
Detect unauthorized changes to protect integrity

Backup and replication systems
Support availability and recovery after loss or attack

Identity and access management (IAM)
Enforces who can see and change data

Industry Standards

ISO/IEC 27001
Frames information security around protecting confidentiality, integrity, and availability

NIST SP 800-53
Control catalog whose safeguards map to the three triad goals

NIST Cybersecurity Framework (CSF) 2.0
Organizes protection, detection, and recovery that serve the triad

Career Relevance

The CIA triad is foundational for SOC analysts, security engineers, GRC analysts, auditors, and architects. Interviewers use it to test whether a candidate can reason about security rather than

just name tools. Privacy and AI governance professionals, the audience AI-Governance-Jobs.com serves, also rely on it to explain why a given control or requirement exists.

Interview Questions

- What are the three parts of the CIA triad, and give a control for each?
- Give an example of a control that protects confidentiality but can hurt availability.
- Which part of the triad does ransomware attack, and how has that changed?
- How would you protect the integrity of a critical financial record?
- Why might availability be the top priority for some systems over confidentiality?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 CISSP (for deeper coverage)

Further Reading

- NIST Glossary: confidentiality, integrity, availability
- NIST Cybersecurity Framework 2.0
- CISA: Cybersecurity Best Practices

Key Takeaways

- The CIA triad is the three core goals of security: confidentiality, integrity, availability.
- Almost every control exists to protect one or more of these properties.
- Protecting one goal can weaken another, so balance is a deliberate choice.
- The triad is a reasoning tool that maps threats and controls to real objectives.
- It is a baseline concept expected in security, GRC, and governance roles.

FAQ

▶ **Is the CIA triad still relevant with modern threats?**

▶ **Are there additions to the CIA triad?**

▶ **How does the triad relate to a framework like NIST CSF?**

Related Careers

RELATED ROLES

Soc Analyst | Grc Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

ISC2 CISSP (for deeper coverage)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **The CIA Triad**
3. Go deeper: Cybersecurity
4. Go deeper: Defense in Depth
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-003 Defense in Depth | CS-009 Core Security Principles | CS-010 Cyber Hygiene | CS-004 Zero Trust