# Security Foundations: The How & Why

## Introduction & Purpose

This session introduces security in a way that goes beyond tools and buzzwords. It is about why security matters and how to think about it strategically. We focus on the CIA Triad — Confidentiality, Integrity, and Availability — as a practical, business-aligned foundation.

Many tools promise security, but the real value lies in building systems that: - Keep data private and only accessible by the right people (Confidentiality) - Ensure data remains accurate and unaltered (Integrity) - Are available and resilient when needed, even under stress (Availability)

## Agenda

1. **Rules of Engagement**  
   Set the tone for the discussion, explain why this matters, and frame security in the customer’s business context.
2. **What is the CIA Triad**  
   Provide a clear breakdown of the three principles and why they matter, supported with real-world examples.
3. **Why It Matters in Practice**  
   Show how the CIA Triad helps set priorities when tools alone cannot solve the problem.
4. **Strategic Conversations, Not Tool Audits**  
   Discuss risk appetite, data value, uptime expectations, and real-life tradeoffs before mapping tools to those priorities.
5. **Integration with Existing Frameworks**  
   Demonstrate how the CIA Triad complements Essential 8, NIST, and Zero Trust without making it a compliance-heavy session.
6. **Next Steps and Call to Action**  
   Outline a clear approach for understanding current posture, identifying critical gaps, and building on the foundation.

## Rules of Engagement

* Stay human and strategic. Conversations should help business leaders feel confident, not overwhelmed.
* Avoid the belief that a tool alone equals security. Focus on principles and outcomes first.
* Use business-centric questions:
  + *What would be the impact if your data was altered by mistake?* (Integrity)
  + *If your systems went down for a day, what would happen to the business?* (Availability)
  + *Who needs access to what and how do we prevent the wrong people from getting in?* (Confidentiality)
* If the conversation becomes too technical too soon, say: *That’s a great topic for a deeper session. Let’s start by confirming the high-level business goal first.*
* When tools are mentioned, link them back to context: *Yes, this tool can encrypt files, but how do we decide which files actually need that level of protection?*

## What is the CIA Triad

| Principle | Definition | Why It Matters in Business Context |
| --- | --- | --- |
| **Confidentiality** | Only authorised users or processes can access or view data. | Prevents leaks of sensitive or proprietary information and protects trust, reputation, and compliance. |
| **Integrity** | Ensures that data remains accurate, consistent, and unaltered. | Prevents damage from accidental or malicious changes and ensures reliable decision-making. |
| **Availability** | Ensures authorised users can access necessary data and services when needed. | Keeps operations running smoothly, reduces downtime, and supports customer trust and business continuity. |

## Why the CIA Triad Still Matters

* It provides clarity in a crowded tool landscape, making the security conversation tactical and tangible rather than theoretical.
* It highlights tensions between principles. For example, strict access for confidentiality can reduce availability, and bandwidth for backups to ensure availability can impact performance.
* It anchors decisions in business priorities rather than chasing features or vendor claims.

## From Concepts to Action

1. **Map your environment to the CIA Triad**
   * What data needs strong confidentiality controls such as encryption or MFA?
   * Where is integrity critical such as transactional systems or audit logs?
   * Where must availability be high such as customer portals or supply chain tools?
2. **Prioritise strategic improvements**
   * Quick wins such as enabling MFA or implementing backups
   * Longer-term investments such as data integrity monitoring or redundant architecture
3. **Tie actions back to frameworks**
   * Use Essential 8 for immediate action planning
   * Show how NIST and Zero Trust can build on a CIA-based posture

## Learning References and Talking Notes

* **Understanding the CIA Triad** (CSO Online)  
  A clear breakdown of confidentiality, integrity, and availability with examples  
  [CSO Online: The CIA Triad](https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html)
* **CIA Triad Fundamentals** (CybersecurityNews)  
  Explains the model in simple terms and its impact on security design  
  [CybersecurityNews: CIA Triad](https://cybersecuritynews.com/cia-triad-confidentiality-integrity-availability/)

## Closing Thought

Security is less about ticking boxes than it is about making systems trustworthy. The CIA Triad acts as a compass, helping us ask the right questions, prioritise what matters to the business, and build resilience rather than relying solely on configurations.