UNIT 5 – WIKI ACTIVITY

Respond to at least two of your peers' contributions in the Wiki. You may find you can answer their questions or provide additional information or clarification or simply compare their results with your own.

Response to peer contribution:

W - What is the difference between a security framework and a regulation?

A security framework provides a structured set of guidelines, best practices, and processes to help organizations manage and reduce cybersecurity risks. Frameworks like NIST CSF or ISO/IEC 27001 are voluntary and offer flexibility in implementation. They guide how an organization can achieve a secure posture. A regulation, on the other hand, is a legal requirement imposed by a government or regulatory body. Regulations (e.g., HIPAA, GDPR, PCI DSS) are mandatory and specify what an organization must do to comply with the law. While frameworks provide guidance, regulations enforce specific rules, and non-compliance can lead to legal penalties or fines. Often, organizations use frameworks to help them achieve compliance with various regulations.

My response:

Great explanation. You've clearly distinguished frameworks from regulations.

However, one small nuance worth adding is that some frameworks (like NIST SP 800-171) are generally voluntary, but become mandatory when written into government contracts (e.g., for contractors working with the US government). This shows the boundary isn't always absolute. Also, PCI DSS is technically an industry standard rather than a regulation, but it's still enforced contractually by the payment card schemes, which gives it regulatory-like weight.

But your main point stands though:

- Frameworks guide **how** to secure systems
- Regulations (or contractually binding standards) dictate **what** must be done

Additional Wiki Contribution:

M - Minimising the burden of multiple frameworks

Conduct a control mapping exercise to align overlapping requirements, for example mapping GDPR's Article 32 (security of processing, such as encryption and access controls) to PCI DSS Requirement 3 (protect stored cardholder data). By reusing the same encryption or access log evidence across both, organisations can cut duplication, ease compliance, and focus resources on strengthening real security.

Key words: Framework, Compliance burden, Overlapping requirements, Control mapping