**Reflective Review**

**1. Analysis of Choices**

**Assignment 1: Backup System Security Analysis and Baseline Assessment**

**For this assignment, I identified key risks such as unencrypted data, inadequate access controls, ransomware, and GDPR compliance requirements. Tools like Veeam for automated backups and Acronis for ransomware protection were chosen due to their reliability and industry recognition (Hanif and Lallie, 2021). Standards such as NIST SP 800-34 and ISO/IEC 27031 provided a framework for contingency planning and data integrity. Prioritising ransomware risks led to the inclusion of HashiCorp Vault for encryption key management (Al-Khayyal et al., 2020).**

**Assignment 2: Executive Summary—Online Shopping System (OSS) Security**

**This assignment addressed vulnerabilities such as weak password policies, outdated software, and insufficient backup strategies. Tools like Commvault ensured backup reliability, while HashiCorp Vault secured sensitive data. GDPR and ISO/IEC 27001 compliance guided recommendations for encryption, failover systems, and access controls (Rolfe et al., 2001).**

**Rationale for Choices**

**Choices were risk-based, prioritising threats with the highest business impact. For example, ransomware risks in Assignment 1 required robust mitigation, while weak password policies in Assignment 2 demanded swift action. Upon reflection, alternative tools like Rubrik or Arcserve could have been explored for broader perspectives on automation and scalability. Comparing such tools would provide better discernment into available solutions (Chetioui et al., 2021).**

**2. Multiple Perspectives**

**Tutor Feedback**

**The module tutor praised my methodical technique to risk identification and alignment with industry standards but emphasised the need for stronger critical analysis and more in-depth academic referencing. This feedback encouraged me to refine my evaluations and strengthen evidence-based justifications for my decisions (Rolfe et al., 2001).**

**Personal Contribution and Peer Support**

**During the module, I helped a peer set up Kali Linux and get familiar with Nmap, BurpSuite and Wireshark for her assignments. This experience reinforced my technical knowledge while improving my ability to explain complex concepts clearly. It highlighted the value of collaborative learning and strengthened my interpersonal skills (Hanif and Lallie, 2021).**

**Personal Perspective**

**Initially, I felt confident in addressing technical vulnerabilities but found compliance and ethical principles more challenging. Feedback motivated me to improve my research and critically reflect on the social and organisational implications of my recommendations. Supporting my peer with Kali Linux also deepened my appreciation for collaborative problem-solving in cybersecurity (Chetioui et al., 2021).**

**Organisational Perspective**

**The assignments emphasize the aligning technical measures with organisational priorities like efficiency and compliance. For instance, automating backups with Veeam while securing key rotations with HashiCorp Vault demonstrated an understanding of balancing operational needs with ethical responsibilities. These lessons prepared me for real-world professional challenges (Al-Khayyal et al., 2020).**

**3. Critique of Artifacts**

**Assignment 1: Backup System Security Analysis**

**Strengths:**

**• Comprehensive identification of risks such as ransomware and unencrypted data.**

**• Clear timelines for evaluating and enforcing strategies.**

**• Alignment with NIST SP 800-34, ensuring practical contingency planning (Hanif and Lallie, 2021).**

**Weaknesses:**

**• Limited depth in linking tools to specific risks. For instance, Splunk’s role in detecting unencrypted data transmissions could have been elaborated.**

**• Over-reliance on automated tools like Veeam without fully exploring their limitations, such as their inability to address complex misconfigurations (Rolfe et al., 2001).**

**Assignment 2: OSS Security Executive Summary**

**Strengths:**

**• Prioritised recommendations for weak passwords and outdated software.**

**• Effective visuals (e.g., compliance charts) to communicate findings clearly.**

**• Focused on GDPR and ISO/IEC 27001 compliance, aligning with legal and ethical standards (Al-Khayyal et al., 2020).**

**Weaknesses:**

**• Recommendations lacked explicit links to findings. For instance, weak password policies could have been tied to real-world exploitation scenarios like credential stuffing attacks.**

**• Limited exploration of alternative recovery strategies, such as decentralised or cloud-based backups (Chetioui et al., 2021).**

**4. Critique of Literature and Action Plan**

**Critique of Literature**

**The assignments referenced standards like GDPR, NIST SP 800-34, and ISO/IEC 27031 alongside academic literature. However, opportunities to integrate recent empirical studies were missed. For example:**

**• While encryption standards were discussed, integrating case studies on real-world ransomware incidents would have enhanced the justification for selecting Acronis.**

**• Comparative analysis of tools (e.g., Rubrik vs. Veeam) would have provided a broader evaluation of available technologies (Hanif and Lallie, 2021).**

**Despite these gaps, sources such as Al-Khayyal et al. (2020) and Chetioui et al. (2021) enriched my understanding of compliance and user trust. Explicitly linking these insights to practical tool applications would further strengthen the review.**

**Action Plan**

**To address these gaps, my Personal Development Plan (PDP) includes the following steps:**

**1. Strengthen Critical Reflection**

**o Journal experiences to deepen reflection on challenges and feedback loops.**

**o Evaluate how feedback shapes my learning and outcomes (Rolfe et al., 2001).**

**2. Expand Research Scope**

**o Incorporate recent case studies and empirical evidence into future assignments.**

**o Use comparative analysis to evaluate strengths and weaknesses of alternative tools (Hanif and Lallie, 2021).**

**3. Apply Skills in Real-World Scenarios**

**o Create simulated environments to test backup strategies and ransomware mitigation tools.**

**o Collaborate with peers on technical setups, drawing on my experience with Kali Linux (Chetioui et al., 2021).**

**4. Enhance Ethical Awareness**

**o Stay updated on GDPR and ISO amendments through workshops and webinars.**

**o Engage in interdisciplinary discussions to understand societal implications of data protection (Al-Khayyal et al., 2020).**

**5. Conclusion**

**Utilising the Reflective Review framework has enabled a thorough evaluation of my educational journey. By investigating carefully my decisions, I pinpointed opportunities for growth. Assisting a colleague with Kali Linux underscored the importance of collaboration and practical problem-solving. My goal is to sharpen critical analysis skills, improve research integration, and understand the relationship between technical skills and ethics, offering a comprehensive perspective on cybersecurity.**

**References**

**• Al-Khayyal, A., Alshurideh, M., Al Kurdi, B. and Aburayya, A. (2020) ‘The impact of electronic service quality dimensions on customers’ e-shopping and e-loyalty via the impact of e-satisfaction and e-trust: A qualitative approach’, International Journal of Innovation, Creativity and Change, 14(9), pp. 257–281.**

**• Hanif, Y. and Lallie, H. S. (2021) ‘Security factors on the intention to use mobile banking applications in the UK older generation (55+)’, Technology in Society, 64, p. 101485.**

**• Chetioui, Y., Lebdaoui, H. and Chetioui, H. (2021) ‘Factors influencing consumer attitudes toward online shopping: the mediating effect of trust’, EuroMed Journal of Business, 16(2), pp. 158–178.**

**• Rolfe, G., Freshwater, D. and Jasper, M. (2001) Critical reflection in nursing and the helping professions: A user’s guide. Basingstoke: Palgrave Macmillan.**