Regulation chosen:

1. GDPR
2. OAIC

Privacy Principles chosen:

1. GDPR1: Lawfulness, fairness and transparency
2. GDPR2: Purpose limitation
3. GDPR3: Data minimisation
4. GDPR4: Accuracy
5. GDPR5: Storage limitation
6. GDPR6: Integrity and confidentiality (security)
7. GDPR7: Accountability
8. APP1: Open and transparent management of personal information
9. APP2: Anonymity and pseudonymity
10. APP3: Collection of solicited personal information
11. APP4: Dealing with unsolicited personal information
12. APP5: Notification of the collection of personal information
13. APP6: Use or disclosure of personal information
14. APP7: Direct marketing
15. APP8: Cross-border disclosure of personal information
16. APP9: Adoption, use or disclosure of government related identifiers
17. APP10: Quality of personal information
18. APP11: Security of personal information
19. APP12: Access to personal information
20. APP13: Correction of personal information

Threats chosen:

1. Accidental Sharing
2. Overworked Cybersecurity Teams
3. Employee Data Theft
4. Ransomware
5. Bad Password Hygiene
6. Bribery
7. Too Much Data Access
8. Fraud
9. Denial

Controls chosen:

1. Identity and Access Management (IDAM)
2. Data Loss Prevention (DLP)
3. Encryption and Pseudonymization
4. Incident Response Plan (IRP)
5. Third-Party Risk Management
6. Policy Management

Mappings chosen:

1. Incident Response Plan (IRP) ==> Accidental Sharing
2. Data Loss Prevention (DLP) ==> Overworked Cybersecurity Teams