GRC Portfolio Project: Security Principles Lab

"Entry-Level Governance, Risk & Compliance Demonstration Project"

Alexandra Bringazen – 6 Feb 2026
Simulated Environment / Educational Project: TryHackMe Security Principles Room

Project Summary

Objective:
To understand and apply foundational information security principles (CIA triad, Parkerian Hexad, defence-in-depth, zero trust, least privilege) and map them to practical organisational controls in a simulated environment.

Skills Used:

- Security principle analysis (Confidentiality, Integrity, Availability)
- Risk identification and differentiation (Vulnerability vs Threat vs Risk)
- Control mapping and implementation planning
- Understanding security models (Bell-LaPadula, Biba, RBAC, MAC, DAC)
- GRC perspective: linking security concepts to business impact and compliance

Tools / Platform Used: TryHackMe simulated lab environment

Learning Outcomes:

- Applied security principles to a fictional mortgage company, GoodHabitat Ltd
- Developed ability to assess layered controls, human error impact, and continuous monitoring
- Learned to document and communicate risks, mitigations, and business impact
- Strengthened understanding of ISO 27001, NIST CSF, and GDPR compliance

Security Principles & Concepts

CIA Triad

- **Confidentiality:** Only authorised users can access data
- **Integrity:** Information remains accurate and unaltered
- **Availability:** Systems and data accessible when needed

DAD (Opposites of CIA)

- **Disclosure:** Breach of confidentiality
- **Alteration:** Breach of integrity
- **Destruction/Denial:** Breach of availability

Parkerian Hexad – six elements:

1. Confidentiality
2. Integrity
3. Availability
4. Possession – control of data by authorised parties
5. Authenticity – verifying source and trustworthiness
6. Utility – ensuring information is meaningful and usable

Core Security Principles Covered:

- Defence-in-Depth
- Zero Trust
- Least Privilege
- Authentication & Non-repudiation
- Vulnerability management

Core Security Principles and Controls for Mortgage broker GoodHabitat Ltd

Principle	Control implemented
Confidentiality	Only authorised users can view sensitive data
Integrity	Checks (hashing and logging ensure accuracy)
Availability	Redundant systems and backups keep services running
Least Privilege	Users get only necessary permissions
Defence-in-depth	Multiple layers of security (firewall + authentication + monitoring)
Zero Trust	Always authenticate access
Authentication	Verify identity before granting access
Non-repudiation	Digital signatures / audit logs to track actions
Vulnerability management	Regular scanning & patching to reduce risks

Control Mapping – GoodHabitat Ltd

CONTROL	SECURITY PRINCIPLE	RESULT ACHIEVED	STATUS
MFA	Zero trust authentication	Only authorized access	Implemented
Data encryption at rest	Confidentiality	Protecting sensitive data from exposure	Implemented
File integrity checking	Integrity	Detect unauthorized changes	Planned
Redundant servers & backups	Availability	Reduce downtime	Planned
User access reviews quarterly	Least privilege	Minimise excessive access	Implemented
Defence layers (firewall + IPS logging)	Defence-in-Depth	Multiple obstacle layers for attacks	Implemented
Digital signing of transactions	Non-repudiation	Proof of action origin	Implemented
Routine vulnerability scanning	Vulnerability Management	Identify weaknesses	Implemented

Security Models

Model	Summary
RBAC (Role Based Access Control)	Access granted based on user role
MAC (Mandatory Access Control)	Access strictly controlled by system policies
DAC (Discretionary Access Control)	Resource owners decide who can access data
Bell-LaPadula	Enforces confidentiality (no read up / no write down)
Biba	Enforces integrity (no write up / no read down)

Business Impact Statement – GoodHabitat Ltd

- **Financial Risk:** Data breaches or security incidents could result in significant financial losses from fraud, remediation costs, or lost revenue.
- **Reputation:** Security failures may damage the company's brand and reduce market confidence in its mortgage services.
- **Compliance/Fines:** Non-compliance with GDPR or FCA requirements could lead to substantial fines and legal penalties.
- **Service Disruption:** Cyber incidents or system failures could interrupt mortgage processing, delaying approvals and payments.
- **Customer Trust:** Breaches of sensitive client data could erode trust, harming long-term relationships and retention.

Policy Example – Access Control Policy Summary

GoodHabitat Ltd enforces a comprehensive **Access Control Policy**, ensuring employees access only systems and data necessary for their role. Role-based permissions are applied and reviewed quarterly, while multi-factor authentication and least privilege principles protect sensitive mortgage information.

Data Classification Levels

Public	Freely available to the public
Internal	Company-internal use
Confidential	Sensitive data with potential harm if exposed
Restricted	Highly sensitive information requiring strict access

Incident Response Summary

- **Detect :** Identify potential security incidents quickly using monitoring and alerting
- **Contain :** Limit the scope and impact of incidents to prevent further damage
- **Recover :** Restore systems and services while preserving evidence for analysis and compliance

Risk Analysis Example (Based on Lab Concepts)

- **Asset :** What you are protecting
- **Threat :** What could go wrong / who could attack
- **Vulnerability** : The weakness that allows it
- **Risk** - The business impact if exploited
- **Mitigation** - Control to reduce likelihood or impact

Risk table - GoodHabitat Ltd

Asset	**Threat**	**Vulnerability**	**Risk**	**Mitigation**
Customer Mortgage Data	Data Breach / Hacker	Weak passwords	Exposure of personal & financial data, GDPR fines	MFA + strong password policy
Mortgage Processing System	Ransomware Attack	Unpatched software	Service downtime, financial loss	Regular patching + backups
Employee Email Accounts	Phishing	Lack of staff training	Account compromise, fraud	Security awareness training + email filtering
Internal File Server	Insider Threat	Excessive access rights	Data theft or alteration	RBAC + quarterly access reviews
Website Portal	DDoS Attack	No traffic filtering	Customers unable to apply for loans	Firewall + DDoS protection service

Lessons Learned / Next step

- **Importance of layered controls:** Multiple layers reduce single points of failure
- **Risk ≠ vulnerability:** Understand likelihood and impact separately
- **Human error is a major factor:** Employee training is critical
- **Continuous monitoring is necessary:** Detect and respond to threats in real time
- **Add SIEM monitoring:** Real-time event analysis improves detection
- **Annual penetration testing:** Identify and remediate vulnerabilities proactively
- **Policy review cycle:** Keep policies updated with evolving threats
- **Security awareness training:** Reduce human error and strengthen overall posture

Compliance Frameworks Highlighted

ISO/IEC 27001	International standard for ISMS and risk-based security control framework
NIST CSF	Voluntary framework for managing and reducing cybersecurity risk (Identify, Protect, Detect, Respond, Recover
GDPR	Legal regulation protecting personal data and privacy with penalties for non-compliance

Outcome:

This project demonstrates the ability to translate security principles into practical organisational controls, evaluate business impact, and communicate security, risk, and compliance effectively — all key skills for an entry-level GRC analyst portfolio.