AI SECURITY IMPLEMENTATION

ACME Finance / ZKC Consultancy

By – Abhi Bhise | Security Architect

Disclaimer

This report is prepared for the ACME Finance CTO and CISO as a high-level security implementation proposal for AI systems across the organization. The document provides strategic direction and planning rather than detailed technical specifications, which will be developed during the implementation phase.

While this proposal outlines a comprehensive approach based on current understanding and best practices in AI security, the final implementation plan may evolve as requirements are further refined and as the AI security landscape continues to develop. Resource allocations, sprint plans, and technical approaches may be adjusted in consultation with ACME Finance stakeholders to address emerging needs and priorities.

The security controls and architectures described represent our recommended approach based on industry best practices and the information available at the time of writing. As AI technologies continue to evolve rapidly, regular reassessment of the security approach is recommended throughout the implementation period.

Contents

Index of figures

Index of tables

Executive Summary

ACME Finance has embarked on an ambitious AI transformation journey following CEO's directive to leverage AI capabilities across all business units. As your strategic security partner, ZKC Consulting has evaluated the current approach and identified significant security risks from the proposed AI implementations with insufficient security governance frameworks.

Our proposed three-month security implementation project addresses these concerns by focusing on two key stakeholder requirements. For your CTO team, we'll develop comprehensive security controls for your selected AI products (RAG-enabled chatbots, co-pilots, and agentic solutions), conduct attack surface analyses, and implement responsible AI practices. For your CISO team, we'll seamlessly integrate Azure Security Co-pilot with your Sentinel migration and develop an automated SOAR solution using Logic Applications and AI agents.

We'll deliver this project through six agile sprints using our proven 4D Framework (Diagnose, Design, Deliver, Defend), with a skilled team of security architects, consultants, and specialists. The total estimated investment is £332,580, including essential technical infrastructure and licensing requirements.

This strategic security implementation will enable ACME Finance to embrace AI innovation while maintaining robust security controls and governance.

Key parameters:

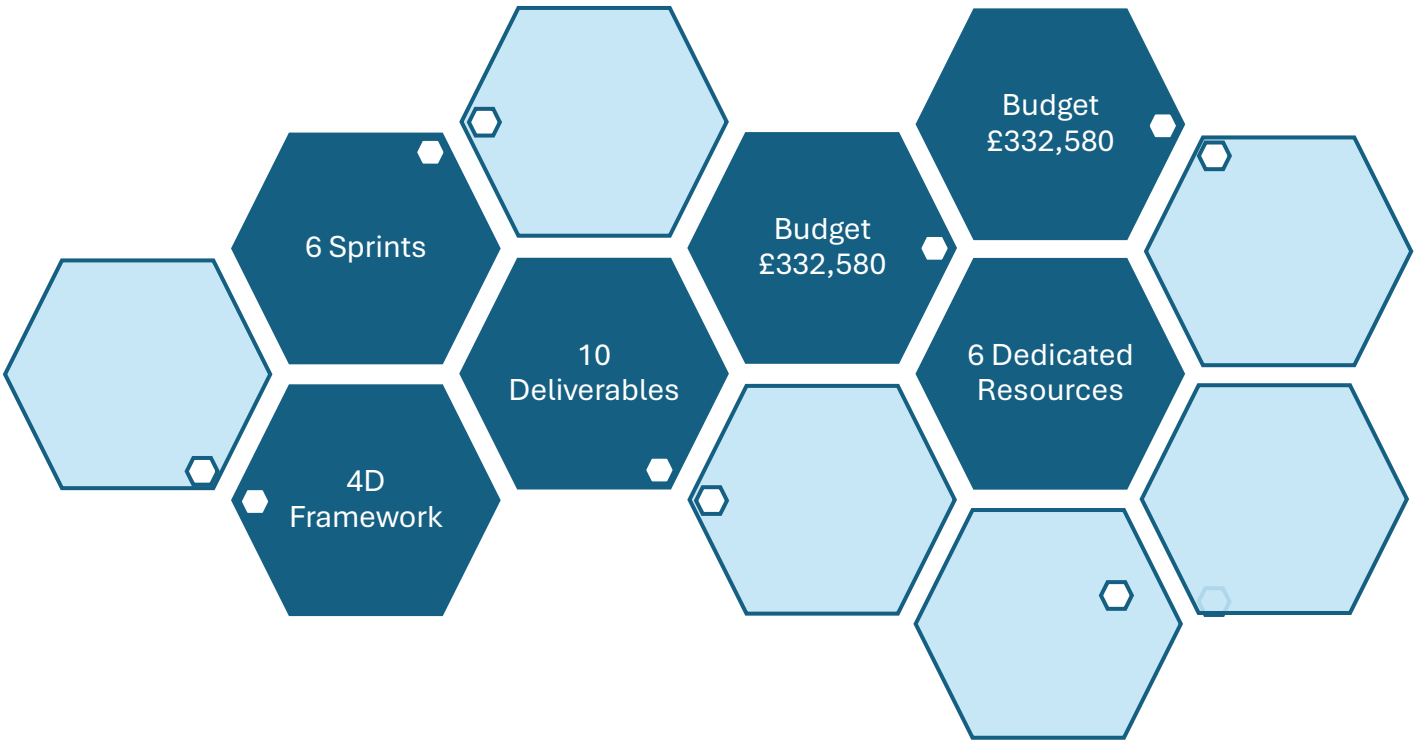

Figure 1 Summary chart

1. Statement of Work

1.1 Client Requirements Understanding

ACME Finance is implementing an enterprise-wide AI transformation programme following CEO's directive to explore AI applications for enhanced operational efficiency and cost reduction. During your recent AI working group meeting chaired by the CTO with participation from the CIO, CISO, CHRO, CFO, and COO significant concerns were raised about the special approach to AI implementation and resulting security gaps.

The consensus reached was that your CISO team should provide security oversight for all AI implementations across the organisation. Given the complexity of AI security and limited internal expertise in this domain, ACME Finance has engaged ZKC Consulting to deliver a comprehensive security project focusing on two key stakeholder groups:

CTO Team Requirements:

- Study and evaluate security controls for three primary AI product categories: RAG-enabled AI chatbots, AI co-pilots, and agentic AI solutions
- Assess changes to internal and external attack surfaces resulting from these AI implementations
- Develop responsible and trustworthy AI security practices tailored to each solution type

CISO Team Requirements:

- Support the transition from LogRythm SIEM to Azure Sentinel with specific focus on security capabilities
- Implement Azure Security Co-pilot for the Security Operations Centre to enhance threat detection and response
- Develop a SOAR solution using Logic Applications and AI agents to automate security incident response

ZKC Consulting will apply our proven 4D Framework (Diagnose, Design, Deliver, Defend) to address these requirements systematically, ensuring comprehensive security oversight while enabling innovation through AI adoption.

1.2 Project Deliverables

Based on our understanding of ACME Finance's requirements, we will provide the following deliverables:

1.2.1 Technical Deliverables

T1. AI Security Control Framework

- A comprehensive set of security controls tailored to each AI product type (chatbots, co-pilots, agentic solutions)
- Technical design specifications for security implementation
- Security testing methodologies for each control category
- Integration guidance with existing security infrastructure

T2. Attack Surface Analysis Report

- Comprehensive threat modelling for each AI implementation type
- Analysis of new attack vectors introduced by AI technologies
- Security architecture diagrams highlighting attack paths and mitigations

T3. Responsible AI Security Implementation Guide

- Guidance for ethical AI boundaries and guardrails
- Implementation guidance for bias detection and mitigation techniques
- Control mechanisms for AI transparency and explainability
- Monitoring solutions for AI behaviour and output validation

T4. Azure Security Co-pilot Deployment

- Technical architecture for Sentinel and Security Co-pilot integration
- Configuration of security templates for common security use cases
- Integration specifications with existing security tools and workflows

T5. SOAR Technical Design

- Architecture design for Logic Apps-based SOAR implementation
- Technical specifications for AI agent integration
- API integration design for security tool orchestration
- Workflow templates for common security scenarios

1.2.2 Non-Technical Deliverables

N1. AI Security Governance Framework

- Security policies specific to AI implementations
- Roles and responsibilities matrix for AI security oversight
- Review and approval workflows for new AI initiatives
- Security compliance checklists for AI projects

N2. Security Operations Procedures

- Updated SOC procedures that include AI capabilities
- Incident response procedures which would include AI co-pilot
- Operational guidelines for AI-assisted security monitoring
- Escalation matrix for AI-related security incidents

N3. AI Security Training Programme

- Training for Security Operations analysts
- Knowledge transfer workshops for security team leaders
- User guides for Azure Security Co-pilot utilisation
- Reference materials for AI security concepts and practices

1.2.3 Hybrid Deliverables

H1. AI Security Risk Assessment Methodology

- Risk assessment tool configurations and templates
- Process documentation for conducting AI security risk assessments
- Risk acceptance and mitigation workflows
- Integration with enterprise risk management framework

H2. AI Security Monitoring Framework

- Technical monitoring solution design and implementation
- Monitoring procedures and operational guidelines
- Alert triage and response workflows
- Performance metrics and dashboard design

2. Technical Solution

2.1 Security Architecture for AI Products

2.1.1 RAG-enabled AI Chatbots Security Architecture

The security architecture for your RAG-enabled AI chatbots will include:

- **Authentication & Authorization Layer**: Azure AD integration
- **Data Protection Layer**: Encrypted data transit and storage with data masking for PII/sensitive information
- **Retrieval Augmented Generation (RAG) Security**: Validation of information sources, preventing unauthorised data access
- **Prompt Injection Prevention**: Input validation controls and prompt sanitisation
- **Audit Logging**: Comprehensive logging of all chatbot interactions for security monitoring

This architecture connects directly with the AI Security Governance Framework (N1) by enforcing the security policies and compliance requirements during chatbot implementation. Here governance framework would provide the policy guardrails while the technical architecture implements those controls.

2.1.2 AI Co-pilot Security Architecture

Your AI co-pilot security architecture will include:

- **Least Privilege Access**: Role-based access controls limiting co-pilot capabilities based on user role
- **Action Validation**: Approval workflows for critical actions recommended by co-pilots (for critical and sensitive tasks)
- **Secure API Integration**: Encrypted connections to backend systems with proper authentication
- **Activity Monitoring**: Detailed logging of co-pilot recommendations and actions taken

This architecture links with the Security Operations Procedures (N2) by enabling appropriate monitoring capabilities that security analysts will utilise during incident response and investigation. The technical controls enable the operational procedures and workflows that your security team will follow.

2.1.3 Agentic AI Security Architecture

For your agentic AI solutions, the security architecture will comprise:

- **Secure Execution Environment**: Isolated runtime environment with controlled system access
- **Permission Management**: Granular permissions for agent actions with approval workflows
- **Data Access Controls**: Just-in-time access to required data sources
- **Agent Activity Auditing**: Comprehensive logging of all agent activities

- **Kill Switch Mechanism**: Emergency disabling capabilities for problematic agents

The agentic architecture ties directly to the AI Security Risk Assessment Methodology (H1) by implementing the technical controls identified during risk assessment activities. As new risks are identified, the architecture can be adjusted to implement appropriate mitigations.

2.2 Azure Security Co-pilot Implementation

2.2.1 Azure Security Co-pilot Integration with Sentinel

The implementation will use Microsoft's security stack integration capabilities:

- **Azure Sentinel as SIEM**: Central logging and alerting platform
- **Security Co-pilot Integration**: Direct linking to Sentinel alerts and logs
- **Custom Connectors**: Integrations with non-Microsoft security tools
- **Secure Authentication**: AAD (Azure Active Directory) based authentication

This implementation connects with the AI Security Training Programme (N3) by providing the technical capabilities that your security analysts will be trained to operate. The training programme content will be directly informed by the technical implementation details of this deployment.

2.2.2 Security Operations Use Cases

The following use cases will be enabled through Security Co-pilot:

1. **Incident Investigation Acceleration**: Automated evidence gathering and correlation
2. **Vulnerability Prioritisation**: Contextual risk assessment of vulnerabilities
3. **Threat Intelligence Analysis**: Pattern recognition and correlation with current events
4. **Alert Triage Automation**: Preliminary analysis of alerts with severity recommendations
5. **Security Documentation Generation**: Automated creation of incident reports and tickets

These use cases provide the technical foundation for the operational procedures detailed in the Security Operations Procedures (N2) deliverable. The technical capabilities would help set SOP (Standard Operating Procedures) that your security analysts will follow during daily operations.

2.3 SOAR Implementation with Logic Apps and AI Agents

2.3.1 Logic App Integration Architecture

The SOAR solution will utilise Azure Logic Apps with the following components:

- **Trigger Management**: Event-based triggers from Sentinel alerts
- **Workflow Management**: Sequential and parallel workflow execution
- **API Connectors**: Pre-built and custom connectors to security tools
- **Approval Workflows**: Human-in-the-loop checks for critical actions

The Logic App architecture connects with the Security Monitoring Framework (H2) by providing the automation engine that implements the monitoring workflows and alert response procedures. The monitoring framework defines what to monitor, while the SOAR implementation automates how to respond.

2.3.2 AI Agent Integration

AI agents will be integrated into the SOAR solution with:

- **Agent Functions**: Predefined functions for common security tasks
- **Decision Support**: AI-driven decision points within workflows
- **Natural Language Processing**: Converting alerts to actionable intelligence
- **Learning Capability**: Continuous improvement based on past incidents

The AI agent integration connects with the AI Security Governance Framework (N1) by operating within the boundaries defined by governance policies. The technical implementation ensures that AI agents remain compliant with organisational security requirements and ethical guidelines.

3. Project Delivery

3.1 Agile Methodology Approach

Our project will utilise a Scrum-based agile methodology with two-week sprints, focusing on delivering incremental value. The approach includes:

- **Sprint Planning**: Defining sprint goals and prioritising backlog items
- **Daily Stand-ups**: 15-minute synchronisation meetings for the team
- **Sprint Reviews**: Demonstrations of completed work to stakeholders
- **Sprint Retrospectives**: Improvement discussions for subsequent sprints
- **Backlog Refinement**: Ongoing prioritisation and clarification of requirements

3.2 Sprint Plan for First Three Months

Sprint 1: Foundation and Architecture (Weeks 1-2)

- **Deliverables**:
    - Initial security architecture designs for AI products
    - Security requirements documentation
    - Project plan finalisation

Justification: Establishing the security foundation is critical for all subsequent work. This sprint focuses on understanding your existing environment and defining the security architecture that will guide all implementations. By prioritising architectural work early, we ensure that subsequent sprints build on solid security principles and avoid costly rework later.

Sprint 2: AI Security Framework Development (Weeks 3-4)

- **Deliverables**:
    - Detailed AI security control frameworks for each product type
    - Attack surface analysis methodology
    - Initial governance framework draft

Justification: Building on the architectural foundation, this sprint develops the specific security controls needed for each AI product type, ensuring a consistent security approach across implementations. The security framework development is sequenced here because it provides essential security guidelines that all subsequent implementations must follow, creating a secure baseline for all AI solutions.

Sprint 3: Azure Security Co-pilot Integration (Weeks 5-6)

- **Deliverables**:
    - Azure Security Co-pilot technical setup
    - Initial integration with Sentinel
    - Security Operations use case configurations

Justification: This sprint focuses on the immediate priority of enhancing your Security Operations capabilities through the implementation of Azure Security Co-pilot, providing early value to your security team. We prioritise this implementation now because it delivers immediate operational benefits to your SOC team while foundational security controls are being finalised in parallel work streams.

Sprint 4: SOAR Solution Design (Weeks 7-8)

- **Deliverables**:
    - Logic App workflow designs
    - AI agent integration specifications
    - Initial playbook implementations

Justification: Building on the Security Co-pilot implementation, this sprint extends automation capabilities through SOAR implementation, further enhancing your security team's operational efficiency. This work sequentially follows the Security Co-pilot integration because the SOAR solution will leverage many of the capabilities established in the previous sprint, creating a more integrated security automation ecosystem.

Sprint 5: Responsible AI Implementation (Weeks 9-10)

- **Deliverables**:
    - Responsible AI security controls implementation
    - Trustworthiness validation methodologies
    - AI security monitoring setup

Justification: With the core security implementations underway, this sprint focuses on ensuring AI implementations adhere to responsible and trustworthy AI principles, addressing ethical considerations. This work is scheduled later in the project timeline because it builds upon the security foundations established in earlier sprints, adding ethical and responsible use layers that complement the technical security controls.

Sprint 6: Training and Handover (Weeks 11-12)

- **Deliverables**:
    - Security Operations training on AI tools
    - Documentation finalisation
    - Knowledge transfer workshops

Justification: The final sprint ensures operational readiness by providing training and complete documentation, ensuring your team can effectively operate and maintain the implemented solutions. This sprint appropriately comes last because it encompasses all the knowledge gained throughout the project and transfers it to your teams who will manage these systems going forward.

4. Resource Requirements

4.1 Resource Allocation per Sprint

Sprints	Resource	Days
Sprint 1: Foundation and Architecture	Enterprise/Security Architect	7
	Security Senior Consultant	10
	Solution Architect	10
	Security Specialist	5
	Senior Project Manager	10
Sprint 2: AI Security Framework Development	Enterprise/Security Architect	10
	Security Senior Consultant	10
	Solution Architect	5
	Security Specialist	10
	Security Operations	5
	Senior Project Manager	10
Sprint 3: Azure Security Co-pilot Integration	Security Senior Consultant	5
	Solution Architect	10
	Security Specialist	10
	Security Operations	10
	Senior Project Manager	10
Sprint 4: SOAR Solution Design	Enterprise/Security Architect	5
	Security Senior Consultant	5
	Solution Architect	10
	Security Specialist	10
	Security Operations	5
	Senior Project Manager	10
Sprint 5: Responsible AI Implementation	Enterprise/Security Architect	5
	Security Senior Consultant	10
	Solution Architect	5
	Security Specialist	5
	Security Operations	5
	Senior Project Manager	10

Sprint 6: Training and Handover	Security Senior Consultant	10
	Security Specialist	5
	Security Operations	10
	Security Service Management	5
	Senior Project Manager	10

Table 1 Resource-Sprint mapping

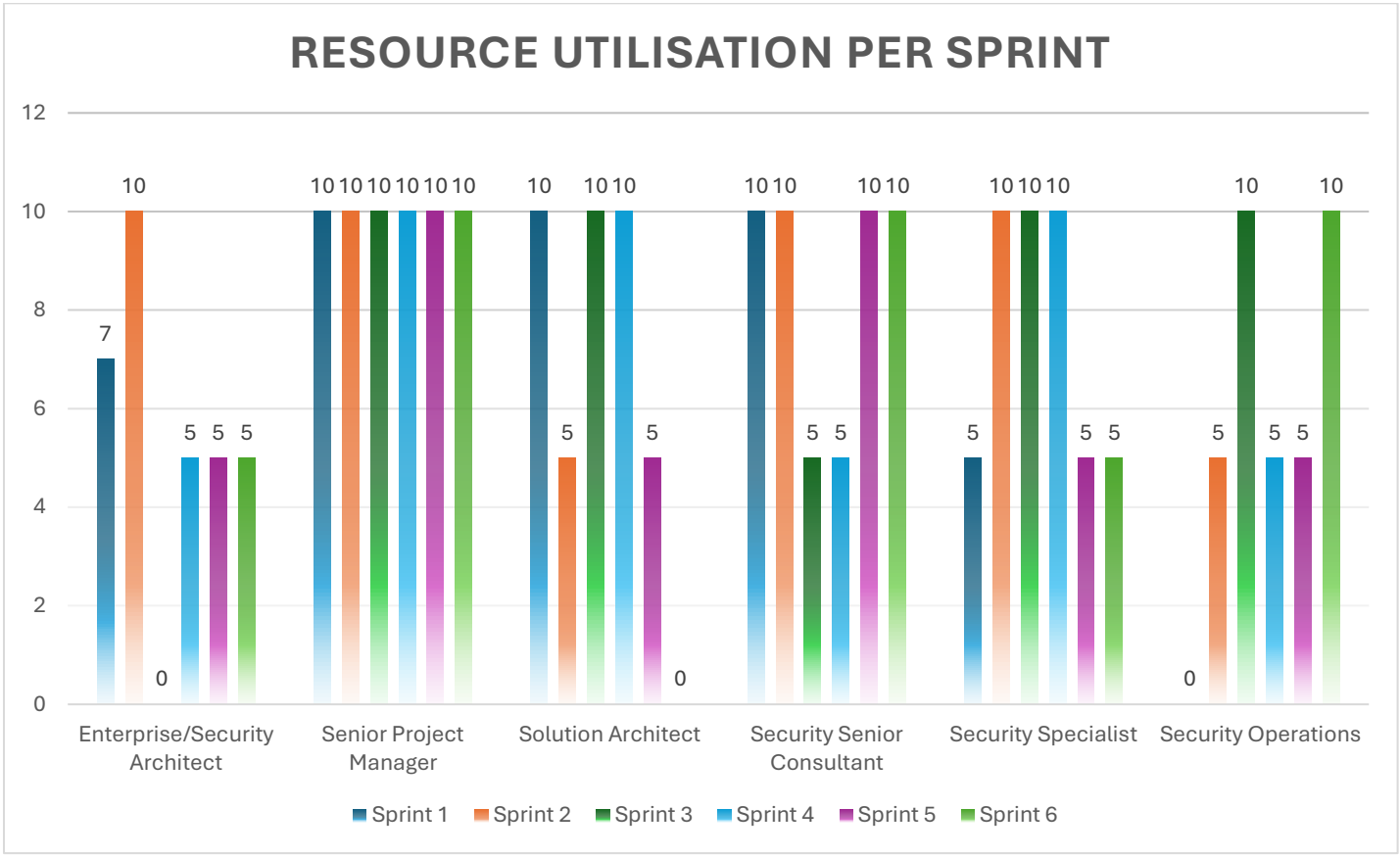

Figure 2 Resource utilisation per sprint

4.2 RACI Matrix

Sprint 1: Foundation and Architecture

Task	Enterprise/ Security Architect	Security Senior Consultant	Solution Architect	Security Specialist	Senior Project Manager	ACME CISO	ACME CTO
Security architecture development	R	A	C	C	I	C	C
Requirements gathering	C	A	R	C	I	C	C
Project planning	C	C	C	C	R	A	I
Environment assessment	C	A	C	R	I	C	C

Table 2 Sprint 1 RACI matrix

Sprint 2: AI Security Framework Development

Task	Enterprise/ Security Architect	Security Senior Consultant	Solution Architect	Security Specialist	Security Operations	Senior Project Manager	ACME CISO	ACME CTO
Control framework development	R	A	C	C	I	I	C	C
Attack surface analysis	A	C	C	R	C	I	I	C
Governance framework draft	A	R	C	C	C	I	C	I
Security testing methodology	C	A	C	R	C	I	I	C

Table 3 Sprint 2 RACI matrix

Sprint 3: Azure Security Co-pilot Integration

Task	Security Senior Consultant	Solution Architect	Security Specialist	Security Operations	Senior Project Manager	ACME CISO	ACME SOC Lead
Security Co-pilot setup	A	C	R	C	I	I	C
Sentinel integration	C	A	C	R	I	I	C
Use case configuration	A	C	C	R	I	C	C
Testing and validation	C	C	A	R	I	I	C

Table 4 Sprint 3 RACI matrix

Sprint 4: SOAR Solution Design

Task	Enterprise/ Security Architect	Security Senior Consultant	Solution Architect	Security Specialist	Security Operations	Senior Project Manager	ACME CISO	ACME SOC Lead
Logic App workflow design	C	C	R	A	C	I	I	C
AI agent integration	C	R	A	C	C	I	C	I
Playbook implementation	I	A	C	R	C	I	I	C
Integration testing	I	C	A	C	R	I	I	C

Table 5 Sprint 4 RACI matrix

Sprint 5: Responsible AI Implementation

Task	Enterprise/ Security Architect	Security Senior Consultant	Solution Architect	Security Specialist	Security Operations	Senior Project Manager	ACME CISO	ACME CTO
Trustworthy AI controls	R	A	C	C	I	I	C	C
Validation methodologies	A	R	C	C	I	I	C	C
Monitoring implementation	C	A	C	R	C	I	I	C
Documentation	C	R	C	A	C	I	I	I

Table 6 Sprint 5 RACI matrix

Sprint 6: Training and Handover

Task	Security Senior Consultant	Security Specialist	Security Operations	Security Service Management	Senior Project Manager	ACME CISO	ACME SOC Lead
Training delivery	A	C	R	C	I	I	C
Documentation finalization	R	A	C	C	I	I	I
Knowledge transfer	A	C	R	C	I	I	C
Operational handover	A	C	C	R	I	C	C

Table 7 Sprint 6 RACI matrix

R – Responsible

A - Accountable

C – Consulted

I - Informed

4.3 Gantt Chart

Deliverable	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5	Sprint 6
Security architecture						
Requirements gathering						
Project planning						
Environment assessment						
Control framework						
Attack surface analysis						
Governance framework draft						
Security testing methodology						
Security Co-pilot setup						
Sentinel integration						
Use case configuration						
Testing and validation						
Logic App workflow design						
AI agent integration						
Playbook implementation						
Integration testing						
Trustworthy AI controls						
Validation methodologies						
Monitoring implementation						
Documentation						
Training delivery						
Documentation finalization						
Knowledge transfer						
Operational handover						

Figure 3 Gantt Chart for the sprint

4.4 Resource Selection Justification

Our resource allocation for this project carefully balances expertise requirements with cost efficiency:

Enterprise/Security Architect: Limited to 32 days across the project, primarily in the early architecture-focused sprints. Their expertise is essential for establishing security foundations but used efficiently due to their higher day rate (£1,200).

Solution Architect: Allocated for 40 days, with heavier concentration in implementation sprints. This role provides critical technical design expertise at a more cost-effective rate (£1,000) compared to the Enterprise Architect.

Security Senior Consultant: Utilized for 50 days across all sprints, providing consistent security leadership throughout the project while maintaining cost efficiency (£800/day).

Security Specialist: Engaged for 45 days on technical implementation tasks, delivering specialized security expertise at a more economical rate (£700/day) than senior consultants.

Security Operations: Allocated 35 days, focused on operational aspects of security implementation, providing hands-on expertise at a cost-effective rate (£600/day).

Senior Project Manager: Consistently allocated 10 days per sprint to ensure proper governance and coordination, justifying their higher rate (£1,000/day) through continuity of leadership.

We deliberately avoided using the more expensive Programme Director (£2,000/day) and Programme Manager (£1,500/day) roles, as the project scope and complexity can be effectively managed by a Senior Project Manager, resulting in significant cost savings of approximately £60,000 over the project duration.

5. Budget and Finance Forecast

5.1 Resource Cost Breakdown per Sprint

Sprint	Sprint Title	Resource	Days	Cost	Total
1	Foundation and Architecture	Enterprise/Security Architect	7	£1,200	£8,400
1	Foundation and Architecture	Security Senior Consultant	10	£800	£8,000
1	Foundation and Architecture	Solution Architect	10	£1,000	£10,000
1	Foundation and Architecture	Security Specialist	5	£700	£3,500
1	Foundation and Architecture	Senior Project Manager	10	£1,000	£10,000
1	**Foundation and Architecture**	**Sprint Total**	**-**	**-**	**£39,900**
2	AI Security Framework Development	Enterprise/Security Architect	10	£1,200	£12,000
2	AI Security Framework Development	Security Senior Consultant	10	£800	£8,000
2	AI Security Framework Development	Solution Architect	5	£1,000	£5,000
2	AI Security Framework Development	Security Specialist	10	£700	£7,000
2	AI Security Framework Development	Security Operations	5	£600	£3,000
2	AI Security Framework Development	Senior Project Manager	10	£1,000	£10,000
2	**AI Security Framework Development**	**Sprint Total**	**-**	**-**	**£45,000**
3	Azure Security Co-pilot Integration	Security Senior Consultant	5	£800	£4,000
3	Azure Security Co-pilot Integration	Solution Architect	10	£1,000	£10,000
3	Azure Security Co-pilot Integration	Security Specialist	10	£700	£7,000
3	Azure Security Co-pilot Integration	Security Operations	10	£600	£6,000
3	Azure Security Co-pilot Integration	Senior Project Manager	10	£1,000	£10,000
3	**Azure Security Co-pilot Integration**	**Sprint Total**	**-**	**-**	**£37,000**

Sprint	Sprint Title	Resource	Days	Cost	Total
4	SOAR Solution Design	Enterprise/Security Architect	5	£1,200	£6,000
4	SOAR Solution Design	Security Senior Consultant	5	£800	£4,000
4	SOAR Solution Design	Solution Architect	10	£1,000	£10,000
4	SOAR Solution Design	Security Specialist	10	£700	£7,000
4	SOAR Solution Design	Security Operations	5	£600	£3,000
4	SOAR Solution Design	Senior Project Manager	10	£1,000	£10,000
4	**SOAR Solution Design**	**Sprint Total**	**-**	**-**	**£40,000**
5	Responsible AI Implementation	Enterprise/Security Architect	5	£1,200	£6,000
5	Responsible AI Implementation	Security Senior Consultant	10	£800	£8,000
5	Responsible AI Implementation	Solution Architect	5	£1,000	£5,000
5	Responsible AI Implementation	Security Specialist	5	£700	£3,500
5	Responsible AI Implementation	Security Operations	5	£600	£3,000
5	Responsible AI Implementation	Senior Project Manager	10	£1,000	£10,000
5	**Responsible AI Implementation**	**Sprint Total**	**-**	**-**	**£35,500**
6	Training and Handover	Security Senior Consultant	10	£800	£8,000
6	Training and Handover	Security Specialist	5	£700	£3,500
6	Training and Handover	Security Operations	10	£600	£6,000
6	Training and Handover	Security Service Management	5	£700	£3,500
6	Training and Handover	Senior Project Manager	10	£1,000	£10,000
6	**Training and Handover**	**Sprint Total**	**-**	**-**	**£31,000**

Table 8 Resource cost breakdown per sprint

5.2 Additional Costs

- Azure Security Co-pilot Licensing: £30,000* (estimated annual cost)
- Logic Apps Consumption: £12,000* (estimated annual cost)
- Testing Environments: £15,000 (one-time setup)
- Documentation and Training Materials: £3,800 (one-time cost)
- **Additional Costs Total: £60,800**

5.3 Total Project Budget

- Sprint Costs Total: £228,400
- Additional Costs: £60,800
- **Total Base Project Budget: £289,200**

5.4 Budget Justification and Contingency

The total project budget of £289,200 is justified based on the complexity of implementing comprehensive AI security controls across ACME Finance's environment within an accelerated three-month timeframe.

Contingency Planning: To account for unforeseen challenges, we recommend adding a 15% contingency to the total project budget:

Base Project Budget: £289,200 + Contingency (15%): £43,380 = **Total Project Budget: £332,580**

These contingency addresses potential risks including:

- Extended integration timelines due to unknown technical complications
- Additional resource requirements if specialized expertise is needed
- Scope refinements as AI security requirements evolve during implementation

The resource allocation reflects a balanced approach between senior strategic resources and hands-on technical specialists. The largest cost component is professional services (79% of base budget), which is appropriate given the specialized expertise required for AI security implementation. The remaining 21% covers essential technical infrastructure and licensing costs that enable the security solution.

This investment should be viewed in context of the potential risk mitigation it provides. A single major security incident involving AI systems could result in financial impacts far exceeding this implementation cost, not including reputational damage and regulatory penalties that could follow.

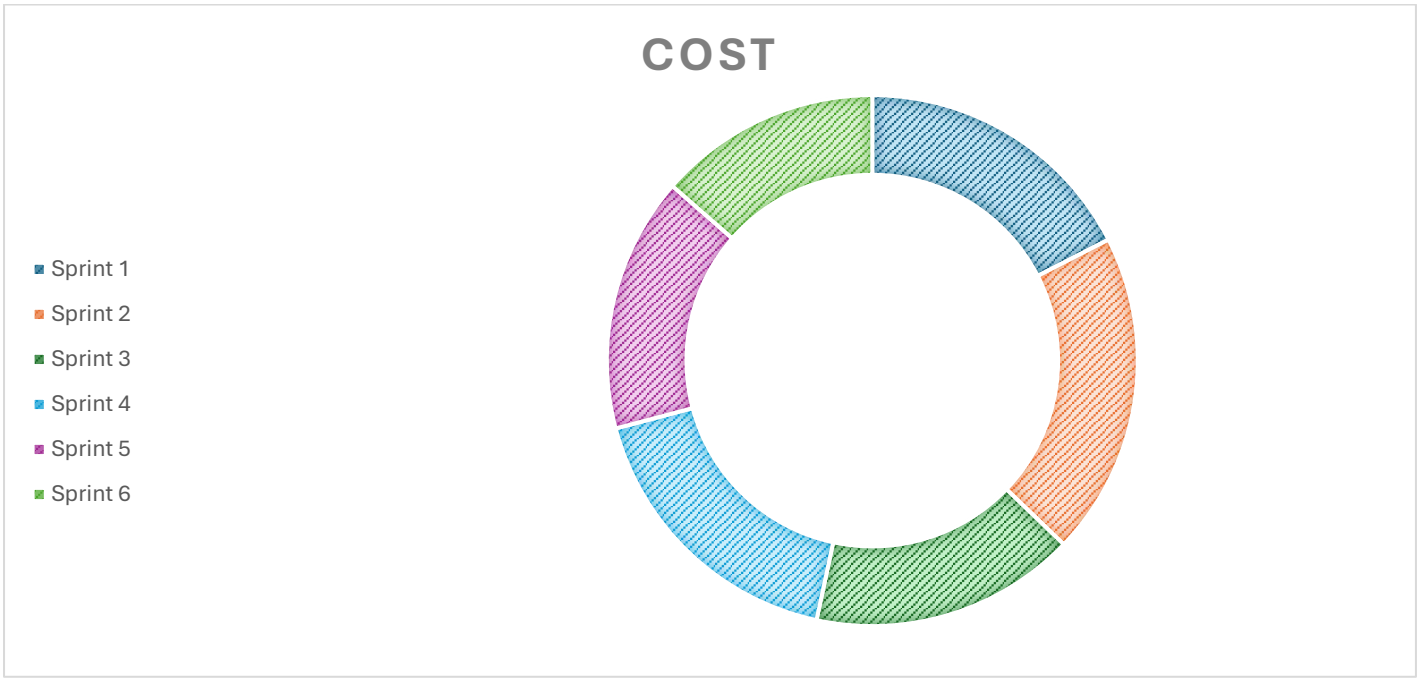

Figure 4 Cost breakdown per sprint

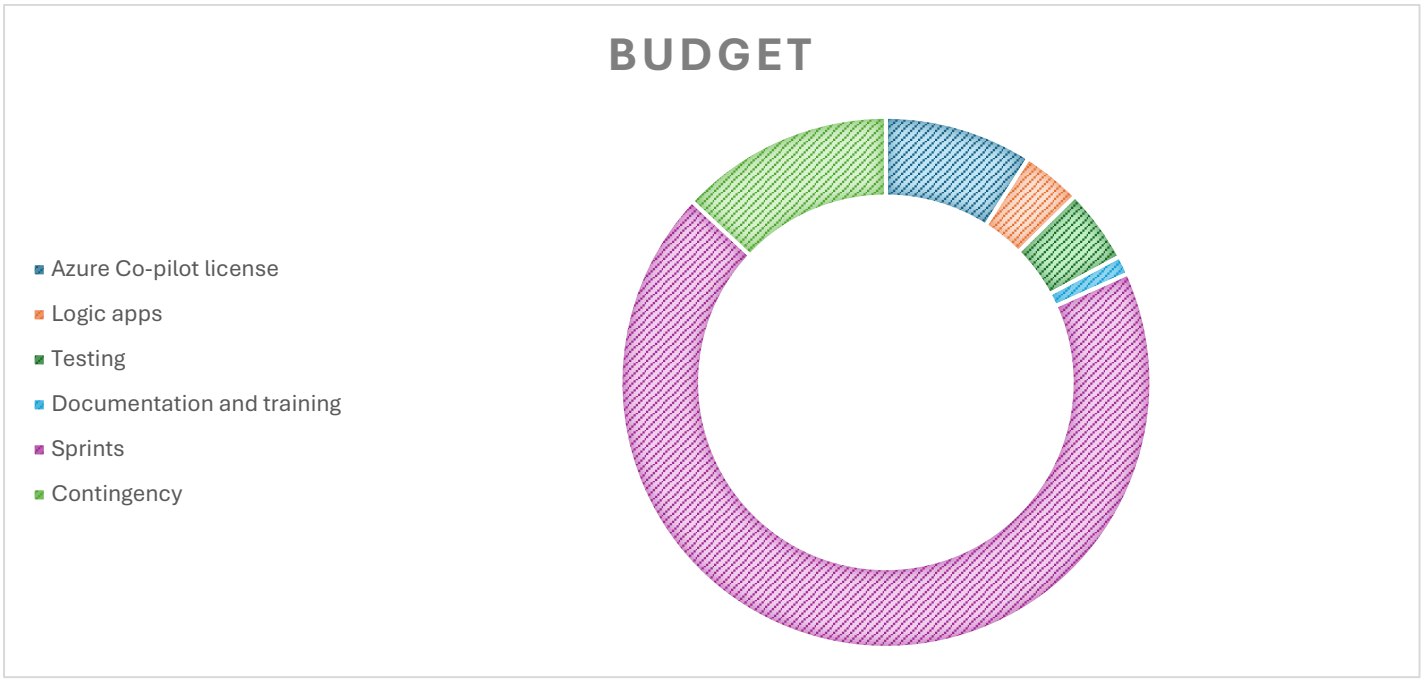

Figure 5 Total budget breakdown

6. Risk Management

6.1 Risk Register

Risk ID	Risk Description	Probability	Impact	Risk Rating	Mitigation Strategy	Risk Owner
R1	Incomplete or changing requirements for AI security controls	Medium	High	High	Early stakeholder engagement, regular review sessions, and incremental delivery approach	Security Senior Consultant
R2	Compatibility issues between Azure Security Co-pilot and existing infrastructure	Medium	High	High	Early assessment of infrastructure, proof-of-concept testing before full deployment	Solution Architect
R3	Limited expertise in AI security within ACME team may impact knowledge transfer	High	Medium	High	Comprehensive training programme, extended handover period, ongoing support arrangements	Security Operations Lead
R4	Resource constraints within ACME teams for participation in project activities	Medium	Medium	Medium	Advance resource planning, flexible scheduling of workshops and meetings	Senior Project Manager
R5	Security vulnerabilities in AI implementations may be discovered during the project	Low	High	Medium	Continuous security testing, rapid remediation process, regular vulnerability assessments	Security Specialist
R6	Data privacy concerns with AI systems accessing sensitive information	Medium	High	High	Robust data governance controls, privacy impact assessments for all AI implementations	Enterprise/Security Architect
R7	Integration complexity between SOAR solution and existing security tools	Medium	Medium	Medium	Phased integration approach, comprehensive testing strategy, fallback procedures	Solution Architect
R8	Resistance to adoption of AI-enhanced security operations workflows	Medium	Medium	Medium	Change management strategy, early user involvement, targeted training sessions	Security Operations Lead

Table 9 Risk Register

6.2 Assumptions

1. ACME Finance has Microsoft licensing to support Azure Security Co-pilot implementation
2. Appropriate access to systems and environments will be provided in a timely manner
3. ACME stakeholders will be available for requirements gathering, reviews, and approvals
4. Basic security controls are already in place for existing systems
5. ACME has established data governance policies that can be extended to AI systems
6. The Security Operations team is willing to adopt new AI-enhanced workflows
7. Required cloud environments are available or can be provisioned quickly
8. Azure Security Co-pilot Licensing and Logic Apps are assumed as pricing would change as per the uses and other factors

6.3 Dependencies

1. Completion of Azure Sentinel migration prior to Security Co-pilot integration
2. Access to Azure environments with appropriate permissions
3. Availability of test environments for solution validation
4. Approval of security policies specific to AI implementations
5. Collaboration with business units implementing AI solutions
6. Knowledge transfer from Microsoft regarding Azure Security Co-pilot configuration best practices
7. Integration API access for existing security tools with SOAR platform

7. Data Security and GDPR Compliance

7.1 Data Security Approach

Our project will maintain customer data security through:

1. **Data Minimisation**: Ensuring AI systems only access the minimum necessary data
2. **Data Classification**: Implementing appropriate controls based on data sensitivity
3. **Access Controls**: Applying least privilege principles to all AI system access
4. **Encryption**: Implementing encryption for data in transit and at rest
5. **Audit Logging**: Extensive logging of all AI system data access
6. **Secure Development**: Following secure development practices for all implementations
7. **Regular Testing**: Security testing throughout the implementation

7.2 GDPR Compliance Measures

To maintain GDPR compliance for AI implementations:

1. **Data Protection Impact Assessments**: Conducted for each AI implementation
2. **Privacy by Design**: Embedding privacy controls in all AI systems
3. **Data Subject Rights**: Ensuring AI systems support data subject request fulfilment
4. **Processing Records**: Maintaining records of all AI data processing activities
5. **Data Retention Controls**: Implementing appropriate data retention policies
6. **Data Transfer Controls**: Ensuring compliance for any cross-border data transfers
7. **Vendor Assessment**: Evaluating third-party AI providers for GDPR compliance

Appendix

A1. Reflection on the exercise

This would be one of the hardest things I have ever done. I worked in the industry not as a consultant but as a security engineer and still was shocked how little I knew about large scale planning. This exercise has really given me a wider view of the details and hard work that goes on behind a companywide project. I would never forget the skills and knowledge I learned doing this exercise and these concepts would be forever engraved in my brain.

I had to consider and change my whole writing style to match the professionalism that is expected when you are presenting a report to a CISO or CTO. I have read and re-read the content again and again to make sure everything is just right. I also had to fact check myself so that I don't introduce any bias or false information into the report. I have researched and learned so many new things while doing this assignment.

The most important realisation was how AI adoption fundamentally changes traditional security paradigms. Unlike conventional security solutions that focus on predictable attack vectors, AI introduces nuanced, emergent risks that require different approaches to threat modelling and control design. As security experts, we must evolve our thinking from purely defensive postures to more adaptive, learning-oriented security frameworks.

Although I have little to no experience doing such reports and limited time to prepare it, I am satisfied with the overall result. There are still many things that could have been improved and the feedback I would get from this assignment would help me figure that out. I generally do care about the grades I get from module assignment but for this module I really care about the feedback I would get and how would I improve my future reports in big organizations.

Thank you for the opportunity to write such a complex report!