ISO 27034 Application Security Framework

AI Applications in Azure AI Foundry with GitHub

Framework Overview

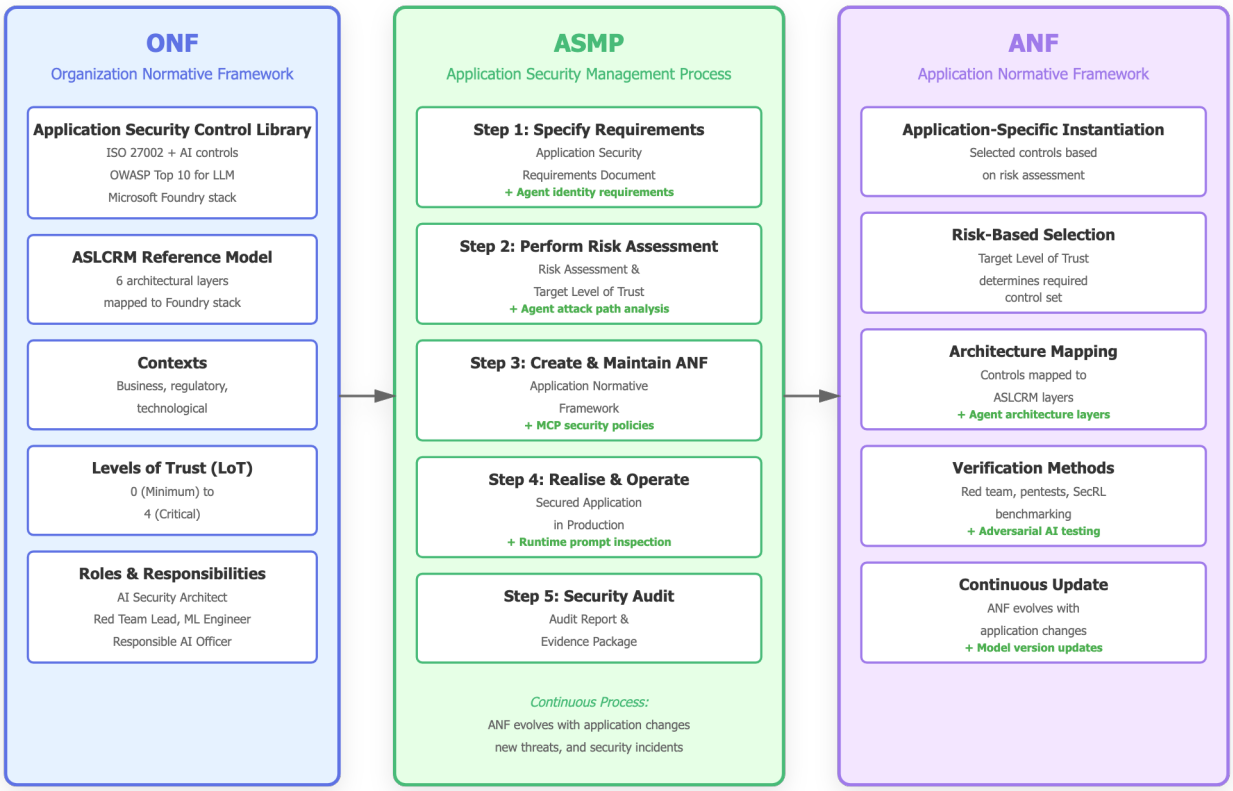
This framework maps ISO/IEC 27034 Application Security to AI systems in Azure AI Foundry with GitHub.

ONF - Organization Normative Framework

ASMP - Application Security Management Process

ANF - Application Normative Framework

New 2025 Controls



Azure AI Foundry: Application Security Units (ASUs)

ASUs are modular security control sets mapped to AI application components. The following table includes controls updated for Microsoft Ignite 2025 and GitHub Universe 2025 announcements.

Control Domain	AI-Specific Implementation	Azure AI Foundry Mapping	Priority
Agent Identity & Access	First-class agent identities with lifecycle policies, conditional access, risk-based controls	Microsoft Entra Agent ID, Agent 365	High AI NEW 2025
Agent Governance	Central registry, MCP server allowlisting, token-based access, sandboxed activity	Agent 365, GitHub Agent HQ, Foundry Control Plane	High AI NEW 2025

Control Domain	AI-Specific Implementation	Azure AI Foundry Mapping	Priority
Build-to-Runtime Security	Continuous feedback loop, campaign launches in GitHub, runtime threats traced to code	GitHub Advanced Security + Microsoft Defender integration	High NEW 2025
AI-Powered Code Security	Automated vulnerability fixes, CodeQL + Copilot, multi-file remediation	GitHub Copilot Autofix (GA), Copilot Code Reviews	High NEW 2025
Prompt Injection Protection	Real-time detection, trusted/untrusted input distinction, document attack blocking	Azure AI Prompt Shield with Spotlighting	High AI NEW 2025
Autonomous Security Operations	AI agents for phishing triage, predictive shielding, automatic attack disruption	Security Copilot agents in Microsoft Defender	High NEW 2025
Agent DLP	Data loss prevention checking for agent prompts before execution	Microsoft Purview DLP for agent prompts	High AI NEW 2025
MCP Security	OAuth 2.1, Resource Indicators (RFC 8707), server vetting, supply chain validation	MCP specification, Azure DevOps MCP Server (GA)	High AI NEW 2025
Agent Threat Detection	Attack path analysis, prompt injection, sensitive data exposure, malicious tool use	Microsoft Defender for AI Agents	High AI NEW 2025
Unified Observability	Single pane for identity, policy, security signals across agent platforms	Foundry Control Plane (Public Preview)	High NEW 2025
Model Security	Model encryption, integrity verification, access control	Azure AI Foundry Model Catalogue, Key Vault	High AI
Secure Development	MLOps pipeline security, model training isolation, CI/CD integration	Azure Machine Learning Pipelines, GitHub Actions	High
Input Validation	Prompt sanitisation, adversarial input detection, injection prevention	Custom validation layers, Azure Functions, Prompt Shield	High AI
Output Encoding	Response filtering, hallucination prevention, unsafe content blocking	Azure AI Content Safety API, custom filters	High AI
Authentication	Model endpoint authentication, API key management, agent identity	Microsoft Entra ID, Managed Identity, Entra Agent ID	High
Authorisation	RBAC for model access, fine-grained permissions, risk-based access	Azure RBAC, Conditional Access, Agent 365 policies	High
Cryptography	Model encryption, secure communication channels, token protection	Azure Key Vault, TLS/mTLS, Customer Managed Keys	High
Error Handling	Safe error messages, no model detail exposure, secure logging	Application Insights, custom handlers	Medium
Logging & Monitoring	Inference logging, drift detection, agent activity tracking, usage analytics	Azure Monitor, Log Analytics, Foundry Control Plane	High
Configuration Management	Model hyperparameters, prompt templates security, MCP configuration	Azure App Configuration, Key Vault	Medium
Vulnerability Management	Model vulnerability scanning, adversarial testing, code scanning with AI fixes	Microsoft Defender, GitHub Advanced Security, CodeQL	High AI

Control Domain	AI-Specific Implementation	Azure AI Foundry Mapping	Priority
Supply Chain Security	Pre-trained model validation, MCP server supply chain, dependency scanning	Azure Container Registry, Dependabot, model catalogue vetting	High AI
Data Protection	Training data privacy, PII handling, data poisoning defence, vector store security	Azure Purview, Information Protection, Private Link	High AI
Business Continuity	Model failover, degraded mode operation, agent redundancy	Azure Site Recovery, Traffic Manager, multi-region deployment	Medium
Compliance	AI regulations (EU AI Act, GDPR), ethical AI compliance, bias auditing	Azure Policy, Compliance Manager, Responsible AI dashboards	High AI

AI-Specific Security Considerations

Novel AI Attack Vectors

- Prompt injection (direct and indirect)
- Model inversion and extraction attacks
- Data poisoning in training pipelines
- Adversarial examples and evasion
- Model card spoofing and supply chain attacks
- Tool poisoning in agent frameworks

Agent-Specific Risks (2025)

- Shadow agents without governance
- MCP servers lacking authentication
- Over-permissioned agent tool access
- Token mis-redemption across services
- Unvetted MCP supply chain components
- Agent sprawl and unclear ownership

Data & Model Governance

- Model versioning and lineage tracking
- Training data provenance and validation
- Bias detection and fairness metrics
- Model explainability requirements
- Drift detection and retraining triggers
- Model update impact assessment

MCP Security Best Practices

- Implement OAuth 2.1 with Resource Indicators (RFC 8707)
- Classify MCP servers as OAuth Resource Servers
- Maintain allowlist of approved MCP servers
- Verify MCP server supply chain and signatures
- Run local MCP servers in sandboxed environments
- Apply least privilege to MCP tool permissions

Implementation Roadmap

Phase 1: Foundation (Months 1-2)

- Establish AI governance framework aligned with ISO 27034
- Deploy Microsoft Entra Agent ID for agent identities
- Configure Agent 365 central registry
- Set up Azure AI Foundry with security baseline
- Implement GitHub Advanced Security + Defender integration
- Deploy Foundry Control Plane for unified observability

Phase 2: Core Security (Months 3-4)

- Enable GitHub Copilot Autofix for code vulnerabilities
- Deploy Azure AI Prompt Shield with Spotlighting
- Implement MCP security controls (OAuth 2.1, allowlisting)
- Configure Purview DLP for agent prompts
- Set up content filtering and output controls
- Establish secure model registry and versioning

Phase 3: Advanced Controls (Months 5-6)

- Deploy Security Copilot agents (Phishing Triage, Predictive Shielding)
- Implement Microsoft Defender for AI Agents
- Configure agent attack path analysis
- Set up adversarial testing and red team exercises
- Deploy AI-specific monitoring and drift detection
- Integrate supply chain security for models and MCPs

Phase 4: Optimisation (Ongoing)

- Continuous security testing with CodeQL and Copilot
- Regular compliance audits for AI regulations
- Agent governance policy refinement
- MCP supply chain monitoring and updates
- Performance optimisation of security controls
- Update ASUs based on emerging AI threats

Critical Success Factors

Technical Considerations

- Implement defence-in-depth strategy for AI systems
- Ensure end-to-end encryption for models and data
- Deploy comprehensive monitoring via Foundry Control Plane
- Automate security testing in CI/CD with GitHub Actions
- Maintain isolated environments for model training
- Enable build-to-runtime security feedback loops

Agent Governance Essentials

- Assign unique identity to every agent (Entra Agent ID)
- Maintain central registry via Agent 365
- Implement MCP server allowlisting and vetting
- Apply risk-based conditional access policies
- Enable human-in-the-loop for high-risk operations
- Track agent activity and audit trails comprehensively

AI-Specific Requirements

- Address unique AI attack vectors (prompt injection, model extraction)
- Implement robust model governance and lifecycle management
- Ensure transparency and explainability in AI decisions
- Monitor for bias and fairness continuously
- Maintain human oversight for critical decisions
- Deploy runtime prompt inspection and filtering

Organisational Alignment

- Establish cross-functional AI security team
- Provide AI security training for developers and engineers
- Define clear roles and responsibilities for agent governance
- Create incident response plans for AI-specific threats
- Regular security awareness for all stakeholders
- Integrate AI security into existing DevSecOps practices

Compliance & Governance

- Map controls to regulatory requirements (GDPR, EU AI Act)
- Maintain comprehensive audit trails for agents and models
- Document AI decision-making processes and rationale
- Regular third-party security assessments
- Establish metrics and KPIs for AI security posture
- Implement continuous compliance monitoring

MLOps as DevSecOps Extension

- Extend CI/CD gates with model and data artefacts
- Version control models like code (signing, provenance)
- Scan training data for injection attacks
- Build-time: CodeQL scans, Copilot Autofix
- Runtime: Prompt Shield, Defender agent triage
- Feedback loops: Runtime threats traced to source code

Key Takeaways

AI AppSec is Additive, Not Parallel

- Traditional AppSec principles still apply to AI systems
- ISO 27034 provides foundation for AI application security

Novel Primitives for AI Era

- Agent identity and lifecycle management
- Runtime prompt inspection and filtering
- Policy-driven tool access for agents
- MCP security and supply chain validation

- Extend existing controls rather than creating separate frameworks
- Leverage ONF, ASMP, and ANF for systematic approach

2025 Security Innovations

- Autonomous security operations with AI agents
- Build-to-runtime continuous feedback loops
- Unified control planes for agent governance
- AI-powered code vulnerability remediation

Future of AI Assurance

- "The next version of AppSec, compiled for machine learning"
- Integration over reinvention - extend ASPM practices
- Shift left with security built into development workflow
- Enable innovation securely, prevent shadow AI adoption