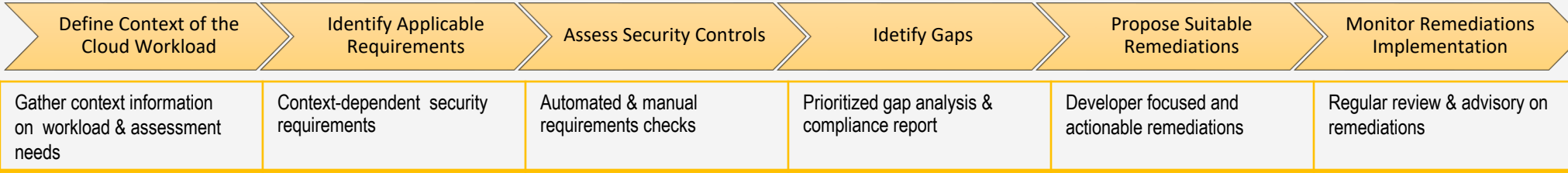


SECURITY ASSESSMENT METHODOLOGY



CONTACT

Spike Reply
www.spike-reply.com
azure.security@reply.de

AZURE SECURITY BEST PRACTICES ASSESSMENT

Technical Analysis	<ul style="list-style-type: none"> Expert-lead assessment and architecture security review Tool-based security checks Manual review and adjustment on tool-based findings
Interviews & Workshop	<ul style="list-style-type: none"> Assess controls not covered in the technical analysis Discuss findings for relevance and criticality within context
Evaluation & Reporting	<ul style="list-style-type: none"> Report security posture and summarize findings & risks Recommend improvements and activities Propose a roadmap to implement recommendations
Final Presentation	<ul style="list-style-type: none"> Present findings and recommendations to the team Clarify questions and define next steps






AREAS OF COMPETENCE IN CLOUD SECURITY

SECURE CLOUD JOURNEY	SECURE CLOUD ARCHITECTURE	CLOUD SECURITY AUTOMATION	SECURE AGILE ORGANIZATION
<ul style="list-style-type: none"> Cloud Security Strategy & Roadmap (Multi-) Cloud Reference Architectures SASE Architectures Data Security 	<ul style="list-style-type: none"> Hybrid & Multi-Cloud Infrastructure Architecture Security Reviews Secure Cloud Native Applications Cloud Trust Services API Management 	<ul style="list-style-type: none"> Continuous Risk & Trust Assessment Automated Security Posture Secure CI/CD Pipelines Secure Container Orchestration and Pipelines 	<ul style="list-style-type: none"> Secure Agile Transformation DevSecOps Organizational Advisory GRC – Agile Alignment

AREAS COVERED BY SECURITY REVIEW

- Network security
- Identity management
- Privileged Access
- Data protection
- Asset management
- DevOps Security
- Logging and threat detection
- Incident response
- Posture and vulnerability management
- Secrets & Key management
- Backup and recovery

AZURE SECURITY

 <p>Assessing security posture of your environments</p> <ul style="list-style-type: none"> Cloud Security Posture Review Infrastructure Analysis against Azure Security Best-Practices Risk-focused remediation and improvement plans 	 <p>Designing and implementing sound cloud networking</p> <ul style="list-style-type: none"> Security best practices for Azure Networking & VNets Setup of Azure native security solutions such as Azure Firewall, NSGs, ASGs, ALB, etc. Establishing sound network architecture and security (e.g hub-spoke architecture)
 <p>Architecting secure Azure deployments</p> <ul style="list-style-type: none"> Setup of Azure tenant using Azure best practices such as Microsoft Azure Well-Architected Framework Review of Azure native application architecture Setup of Azure API Management service Adoption of Zero-trust approach to security design 	 <p>Optimally operating and monitoring Azure deployments</p> <ul style="list-style-type: none"> Azure native logging Log collection on premise and multi-cloud Comprehensive monitoring and alerting using Azure Monitor Setup of Azure Sentinel
 <p>Securing native compute and storage services</p> <ul style="list-style-type: none"> Securing VMs and Blob Storage AKS & Serverless applications security Securing Azure WebApps, Azure native Databases and other IaaS & PaaS solutions 	 <p>Achieving Azure security governance</p> <ul style="list-style-type: none"> Role and Administration Concepts Security management and compliance via Microsoft Defender Continuous Risk & Compliance