Managed Security Operations Centre (SOC)

Service Definition Document

risual Ltd

www.risual.com

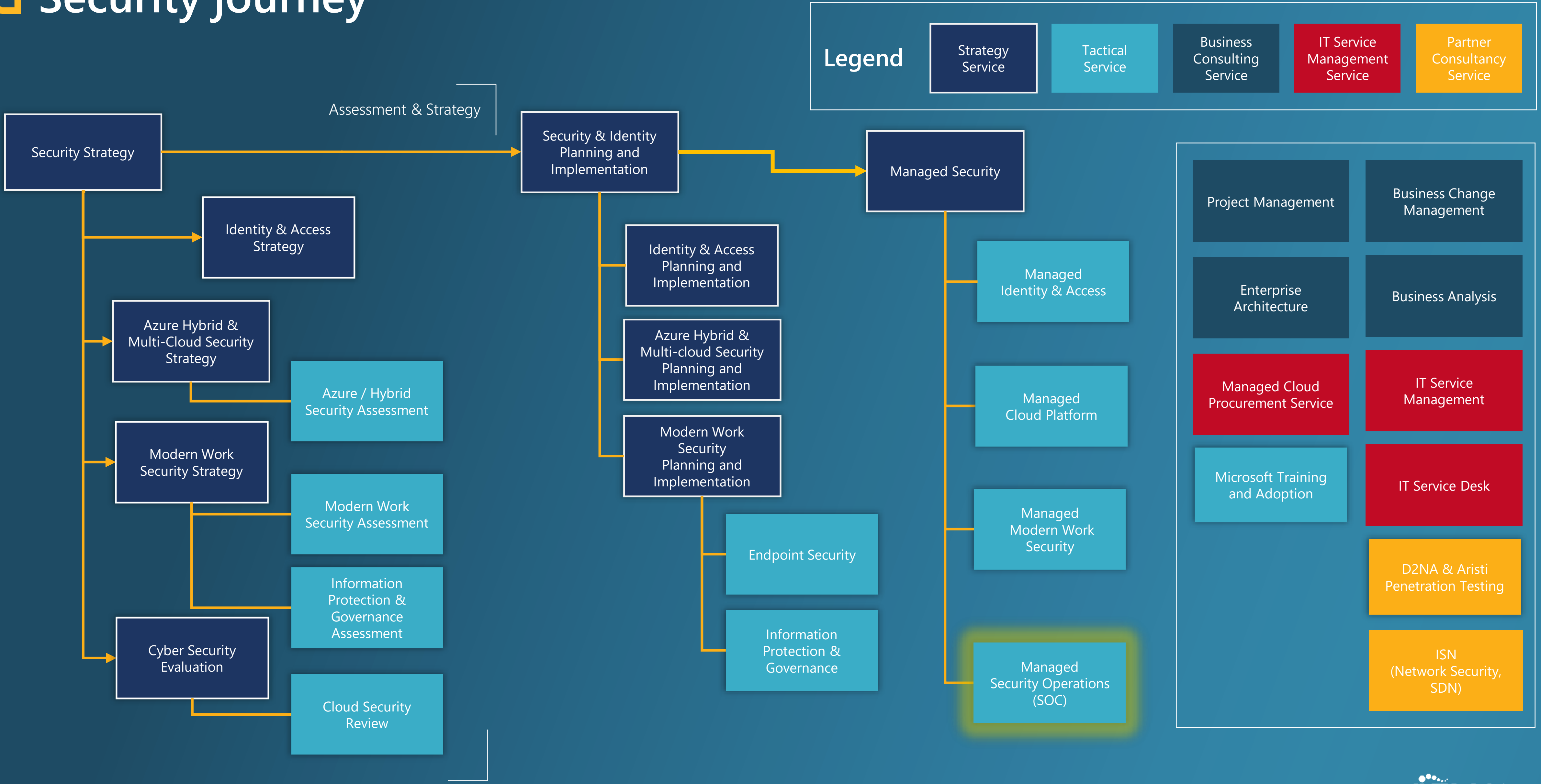
Security is in our DNA

Founded by EMEA's first Security MVP who instilled a 'secure from day one' approach.

Microsoft Gold Partner across 15 categories (including Security) and an Azure Expert MSP; we're in the top 0.05% of MS partners globally.

ISO27001 and Cyber Essentials Plus accredited organisation, NPPV-3 vetted and security cleared UK-based permanent staff.

Security journey



Legend

Strategy Service

Tactical Service

Business Consulting Service

IT Service Management Service

Partner Consultancy Service

Assessment & Strategy

Security Strategy

Identity & Access Strategy

Azure Hybrid & Multi-Cloud Security Strategy

Azure / Hybrid Security Assessment

Modern Work Security Strategy

Modern Work Security Assessment

Information Protection & Governance Assessment

Cyber Security Evaluation

Cloud Security Review

Security & Identity Planning and Implementation

Identity & Access Planning and Implementation

Azure Hybrid & Multi-cloud Security Planning and Implementation

Modern Work Security Planning and Implementation

Endpoint Security

Information Protection & Governance

Managed Security

Managed Identity & Access

Managed Cloud Platform

Managed Modern Work Security

Managed Security Operations (SOC)

Project Management

Business Change Management

Enterprise Architecture

Business Analysis

Managed Cloud Procurement Service

IT Service Management

Microsoft Training and Adoption

IT Service Desk

D2NA & Aristi Penetration Testing

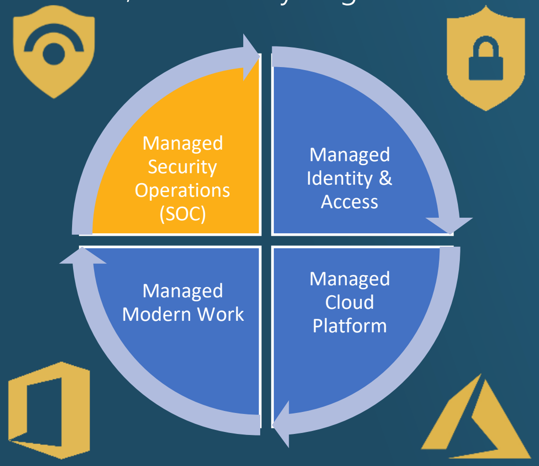
ISN (Network Security, SDN)

Managed Security Operations (SOC)

Description

Incorporating advanced threat intelligence, vulnerability scanning and security analytics, risual's managed security information and event management (SIEM) service includes incident prevention, detection, automated and manual response. Our Managed Security Operations is based on Microsoft Sentinel that can collect events cross all users, devices, applications, and infrastructure, both on-premises and in multiple clouds, coupled with risual's Microsoft accredited security expertise.

We have broken down our SOC service into three levels, Silver, Gold and Platinum, to ensure you get the service you need.



Features

- Investigation across Windows/Linux OS, Office 365, Common Event Forwarding, Syslog and REST-API support networking services, On-premises and multiple Cloud services.
- Detects threats and hunt for suspicious behaviour across a range of Microsoft and non-Microsoft products.
- Managed security incident detection and response reporting to your internal teams or action taken on risual managed services.
- 24x7x365 proactive monitoring and event diagnosis.
- Maintains alignment to the latest cyber security trends and patterns.
- Provide continuous monitoring and remediation (only if agreed by the client)
- All staff UK-based, NPPV-3 and security cleared.
- We can integrate with your IT management systems.

Benefits

- Different service models allow you to get the service you need.
- Delivered by a member of the Microsoft Intelligent Security Associated (MISA) partner.
- Aligned to the 14 NCSC Cloud Security Principles.
- Delivers a comprehensive security operations service.
- Rapid deployment for SIEM capability.
- Allows for stable, consistent & secure delivery of IT services.
- Proactive monitoring and 24x7x365 incident management.
- Utilises security features related to your Microsoft licensing models.
- Underpinned by our ISO 27001 Information Security and Cyber Essentials Plus accreditations.
- Provide monthly/weekly reports of the compliance status.
- Available via multiple procurement frameworks, G-cloud, DOS v5, Bloom, North of England CPC, NHS SBS and Cyber Security Services 3.

Managed Security Operations (SOC) Service Levels

Service Description	Silver	Gold	Platinum
Security Operations Readiness Assessment risual will discover and review your current IT infrastructure, data repositories, cyber security and compliancy requirements against priorities. risual will gain an understanding of client's current Microsoft licensing and therefore which security products are available.	✓	✓	✓
Sentinel Deployment Initial setup and configuration of Microsoft Sentinel core components, and connectivity into risual's monitoring platform.	✓	✓	✓
Service Establishment Configuration of the required SIEM and SOAR capabilities using standard log sources, dashboards and automation.	✓	✓	✓
Managed Sentinel Service Ongoing management of the core Microsoft Sentinel service components, service reporting and cost analysis.	✓	✓	✓
Sentinel Health Check Annual assessment of the Microsoft Sentinel implementation to ensure it continues to meet requirements.	✓	✓	✓

Managed Security Operations (SOC) Service Levels

Service Description	Silver	Gold	Platinum
Monitoring target assessment Identify which monitoring targets should be included to meet the SOC monitoring scope objectives.	✗	✓	✓
risual managed SIEM / SOAR Service Using Sentinel risual will monitor, alert, report and provide advice on the deployment of the of the escalation matrix/incident workflows which are integrated into the client's incident management system.	✗	✓	✓
Monthly SoC Review Regular review the service performance, threat detection statistics, management of incidents. Review of IT infrastructure, detected threats, service risk and changes to requirements and data collection	✗	✓	✓
Service Development Creation of service enhancements base on client's non-standard requests/requirements, or developments in cyber threats. (non-standard log-sources, bespoke dashboards or automation)	✗	✓	✓
Urgent security information notifications Information alerts on emerging threats, zero-day vulnerabilities and urgent security good practice as is made available to the SOC.	✗	✓	✓

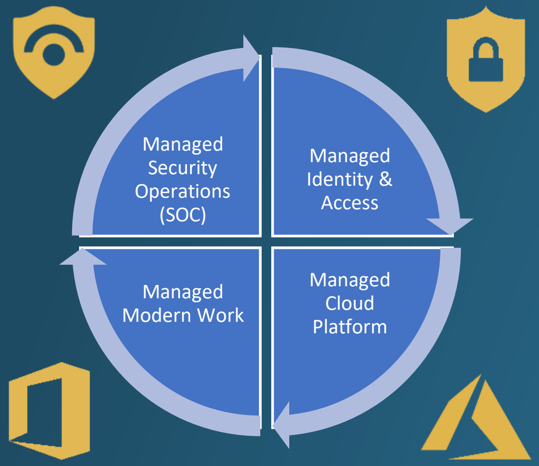
Managed Security Operations (SOC) Service Levels

Service Description	Silver	Gold	Platinum
Vulnerability scanning Support for regular vulnerability scanning	✗	✗	✓
Threat Hunting Support for threat hunting using Microsoft's standard tools	✗	✗	✓
Response Assistance Assistance from risual to co-ordinate and participate in the response to alerts where significant vulnerabilities have been identified.	✗	✗	✓
Incident Response Assistance Assistance in the containment, interim protective measures and remediation following security incidents.	✗	✗	✓

Managed Security

Description

Incorporating advanced threat intelligence, vulnerability scanning and security analytics, risual's fully managed Security includes incident prevention, detection, automated and manual response. Our offering incorporates cloud and on-premises infrastructure, Modern Work (Microsoft 365) and end points covering managed mobile and Windows 10 devices.



Features

- Delivered by Microsoft certified security consultants and engineers.
- Security incident detection and response for cloud and on-premises environments.
- "Single version of the truth" across all Microsoft products/services.
- Maintains your security strategy and supports your compliancy goals
- Maintains alignment to the latest cyber security trends and patterns.
- Includes a proof of concept, with eligible Microsoft funding.
- All staff UK-based, NPPV-3 and security cleared.
- Provide monthly/weekly reports of the compliance status.
- Dedicated Service Delivery Manager for the service.

Benefits

- Delivered by a member of the Microsoft Intelligent Security Associated (MISA) partner.
- Delivered by an Azure Expert MSP accredited Microsoft partner.
- Aligned to the 14 NCSC Cloud Security Principles.
- Delivers a comprehensive security information and event management (SIEM) service.
- Rapid deployment for full, low-cost SIEM capability.
- Allows for stable, consistent & secure delivery of IT services.
- Allows organisations to adopt a zero-trust security approach.
- Proactive monitoring and 24x7x365 incident management.
- Uses all the security features related to your licensing models.
- Covers Azure, Microsoft 365 and Dynamics 365 services.
- Underpinned by ISO 27001 Information Security and Cyber Essentials Plus.
- Available via multiple procurement frameworks, G-cloud, DOS v5, Bloom, North of England CPC, NHS SBS and Cyber Security Services 3.

Who we are

Microsoft Experts since 2005, we have deep product knowledge across Microsoft technologies and a broad range of experience across industry. Born from a belief that technology can change the world in sustainable ways that drive positive social and societal change, we endeavour to learn, develop and invest in our people and communities, delivering world class services that create value and opportunities for all.

UK-based business & technology services organisation, offering consultancy, managed services, training & adoption, education, and apprenticeships for cloud technologies.

Transforming the workplace through the introduction, adoption and strategic management of Microsoft technologies.

Accredited to ISO 27001, ISO 20000, ISO 9001, Cyber Essentials, Cyber Essentials Plus, and members of the NCSC's Cyber Security Information Sharing Partnership (CiSP).

Microsoft Gold Partner across 15 categories
We are a Microsoft Azure Expert MSP
and a member of the Microsoft Intelligent Security Association (MISA)

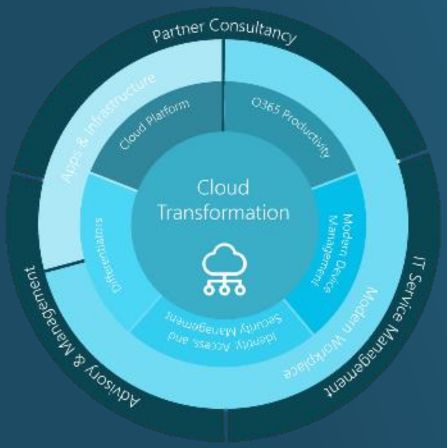
An elite Microsoft Partner, we also have 8 Microsoft advanced specialisations, validating our extensive capabilities in specific solution areas.

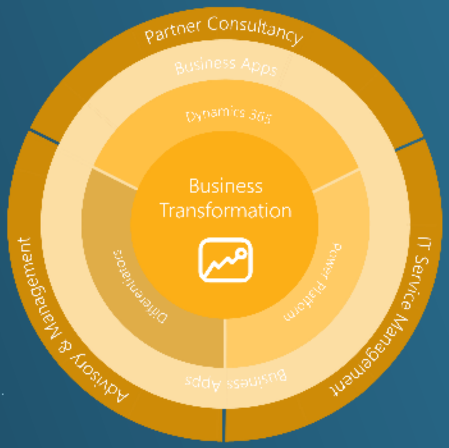
We're driven by a real purpose to introduce sustainable change and drive positive social impact, by increasing the opportunities available to young and disadvantaged people.

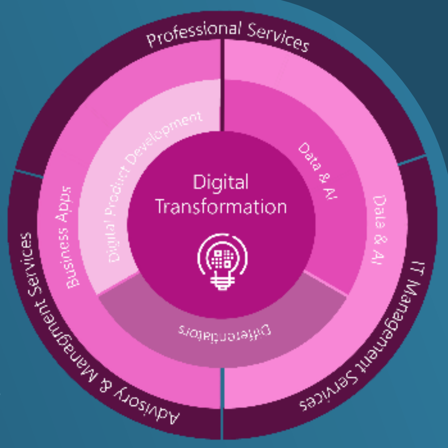
Gold Microsoft Partner Azure Expert MSP · Member of Microsoft Intelligent Security Association Microsoft · The Open Group Open Certified · PRINCE2 · AgilePM · Prosci · SAFe · ITIL · Cyber Essentials · Investors in People · bsi. ISO/IEC 27001 Information Security Management · bsi. ISO/IEC 20000-1 Information Technology Service Management · bsi. ISO 9001:2015 Quality Management

What we do

We are recognised by Microsoft as one of the only partners who deliver a range of services across all three Microsoft clouds; Azure, Dynamics 365, and Microsoft 365. Whilst we have hybrid cloud capabilities and skills with AWS and Oracle, our deep relationship with Microsoft has had a strategic influence on our organisation and the services we deliver since the day we were founded. We are experts in transformation and see transformation in three ways; Cloud, Business and Digital.







Cloud Transformation is about tools and technology, often IT-led it focuses on the platform with Azure, and Modern Workplace through Microsoft 365 services. Cloud Transformation is an enabler and in order to deliver real value, business transformation is required.

Business Transformation is about re-engineering internal services to better serve the business, focusing on business applications, processes and productivity, through Dynamics 365 and the Power Platform.

Digital Transformation relates to external interfaces with clients/citizens/students and enters the domain of disruptive innovation focusing on replacing or complimenting existing services through digital product development.

All three service portfolios span: business and technical consulting, managed services, training & adoption, apprenticeships, and data & AI.

We live by our values of **honesty, openness and trust,** and we embed these values into everything we do, from delivering new and exciting business and technology services/solutions, through to the charity work we regularly undertake within our communities.

advisory
assessment | strategy

consulting
plan | implement

services
optimise | support

skills
develop | adopt

solutions
sector | software

Security services

Identity & Access Management

We help our clients take care of day to day operations with confidence, leveraging their identities to secure and manage user access to applications and services from any device, anywhere. We provide secure, integrated and efficient identity & access management solutions, that are fit for purpose, with managed services options available to provide peace of mind that your identities are regularly optimised for performance and security.

Azure, Hybrid and Multi-Cloud

We help our clients design, deploy and support the secure foundations their businesses need to thrive in the cloud. Securing applications and services to build trust through built-in features and partner solutions. Capabilities extend beyond day to day operations, to applications, storage, networking, compute and Identity, enabling you to scale with confidence, knowing that your applications and services are secure, end-to-end.

Modern Work

We help our clients combat emerging threats and mitigate risks by securing the identities, data and devices they use to access cloud services. Our services align to zero trust principles and focus on providing users with the support and confidence they need when working in a world of hybrid work. We help our clients strengthen cybersecurity through modern threat detection and response approaches that drive operational resiliency.

risual

ACCELERATE YOUR TRANSFORMATION

AND PROTECT AGAINST EVOLVING CYBERSECURITY THREATS WITH RISUAL

Contact Us: ☎ 0300 303 2044 ✉ enquiries@risual.com 🌐 www.risual.com

www.risual.com