Managed Security Operations Centre (SOC)

Service Definition Document

risual

Security is in our DNA

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

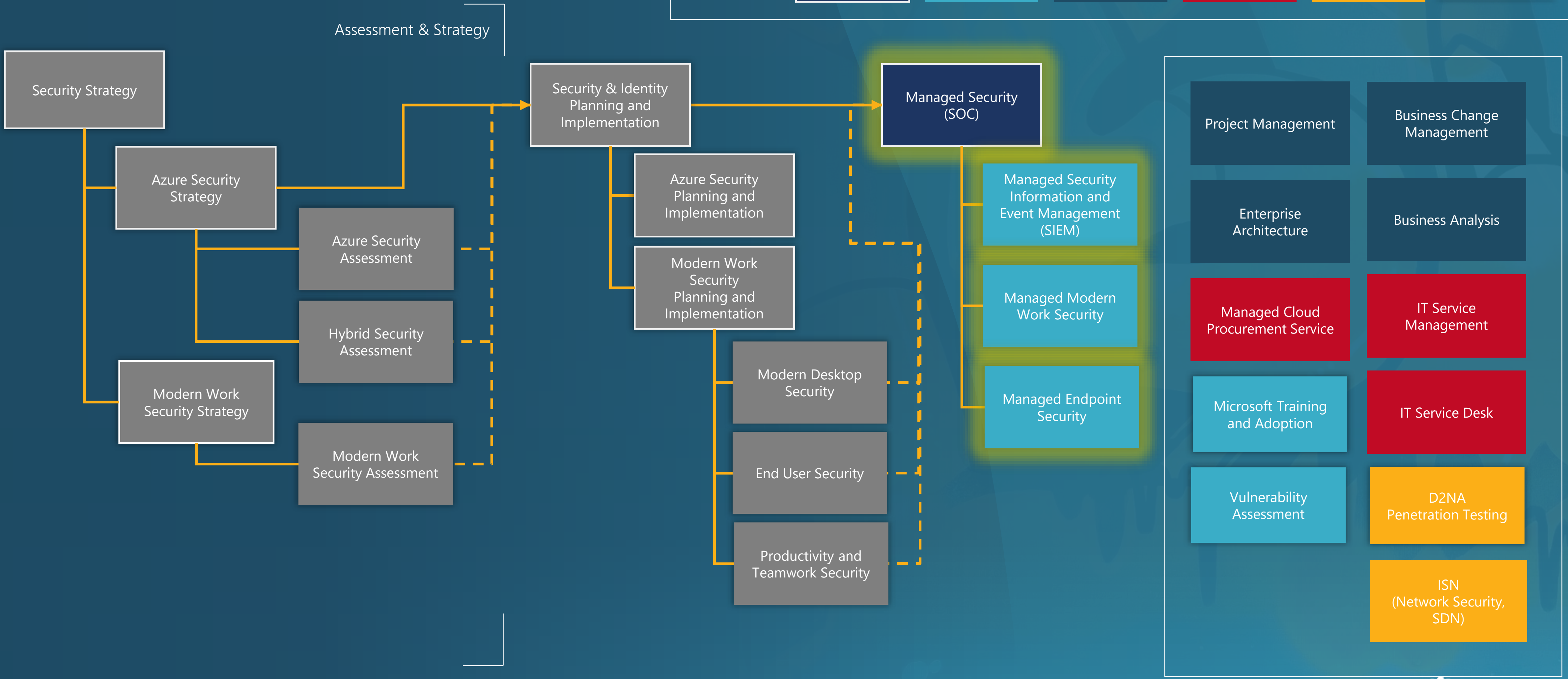
Microsoft Gold Partner across 15 categories (including Security) and an Azure Expert MSP; we're in the top 0.05% of MS partners globally.

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

Microsoft Security & Identity

Legend

- Strategy Service
- Tactical Service
- Advisory Management Service
- IT Service Management Service
- Partner consultancy Service
- Unique risual Service



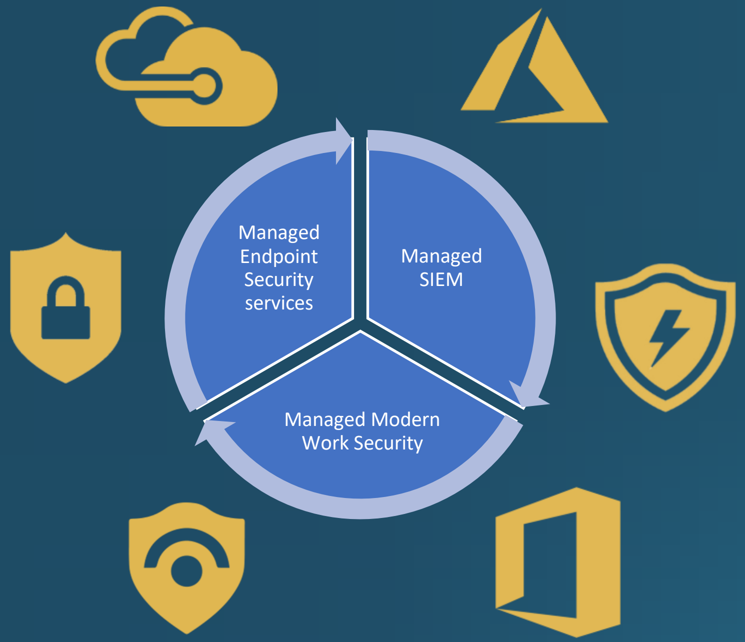
Assessment & Strategy
Security Strategy
Azure Security Strategy
Azure Security Assessment
Hybrid Security Assessment
Modern Work Security Strategy
Modern Work Security Assessment
Security & Identity Planning and Implementation
Azure Security Planning and Implementation
Modern Work Security Planning and Implementation
Modern Desktop Security
End User Security
Productivity and Teamwork Security
Managed Security (SOC)
Managed Security Information and Event Management (SIEM)
Managed Modern Work Security
Managed Endpoint Security
Project Management
Business Change Management
Enterprise Architecture
Business Analysis
Managed Cloud Procurement Service
IT Service Management
Microsoft Training and Adoption
IT Service Desk
Vulnerability Assessment
D2NA Penetration Testing
ISN (Network Security, SDN)

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

MANAGED SOC

Description

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


Managed Endpoint Security services
Managed SIEM
Managed Modern Work Security

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 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

MANAGED SIEM

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 SIEM is based on Microsoft Azure 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.

Features

- Delivered by Microsoft certified security consultants and engineers.
- 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

- 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.
- Proactive monitoring and 24x7x365 incident management.
- Uses all the security features related to your 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 MODERN WORK SECURITY

Description

As more data and services move to the cloud the controlling the security risks and threats can challenging. Our service takes over the task for your organisation and provides clear actionable activities.

Our Managed Modern Work Security utilises features of Microsoft's Defender for Office, Defender for Identity and Cloud App Security as well as native security features in Office 365, coupled with risual's Microsoft accredited security expertise to provide a managed security service.

Features

- Delivered by Microsoft certified security consultants and engineers.
- Detects threats suspicious behaviour across Microsoft Office 365 and non-Microsoft cloud services.
- 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.
- All staff UK-based, NPPV-3 and security cleared.
- Provide continuous monitoring and remediation (only if agreed by the client)
- Feed into clients existing SOC or our managed SOC service.
- Manages change of security services and implements new policies.

Benefits

- Delivered by an Azure Expert MSP accredited Microsoft partner.
- Aligned to the 14 NCSC Cloud Security Principles.
- Delivers comprehensive security management for Microsoft Office 365
- 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.
- Underpinned by our ISO 27001 Information Security and Cyber Essentials Plus accreditations.
- Provide monthly/weekly reports of the compliance status
- Accelerate your organisations compliance making the most of security investments.
- Available via multiple procurement frameworks, G-cloud, DOS v5, Bloom, North of England CPC, NHS SBS and Cyber Security Services 3

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

risual

MANAGED ENDPOINT SECURITY

Description

As end users demand increases to access work from any device at any time, maintaining a secure end point is now key.
The Managed Endpoint Security service is based on Microsoft Defender for Endpoint and Microsoft Endpoint Manager coupled with risual's Microsoft accredited security expertise to provide a managed service for Windows 10, iOS and Android devices.

Our service takes over management of device security for your organisation and provides clear actionable activities.

Features

- Delivered by Microsoft certified security consultants and engineers.
- Includes Windows 10, iOS and Android (contact us for specific version support)
- Detects threats and endpoint misconfiguration vulnerabilities.
- 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.
- Manages change of existing security features and supports the implementation new features.

Benefits

- Delivered by an Azure Expert MSP accredited Microsoft partner.
- Aligned to the 14 NCSC Cloud Security Principles.
- Proactive monitoring and 24x7x365 incident management.
- Uses all the security features related to your 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

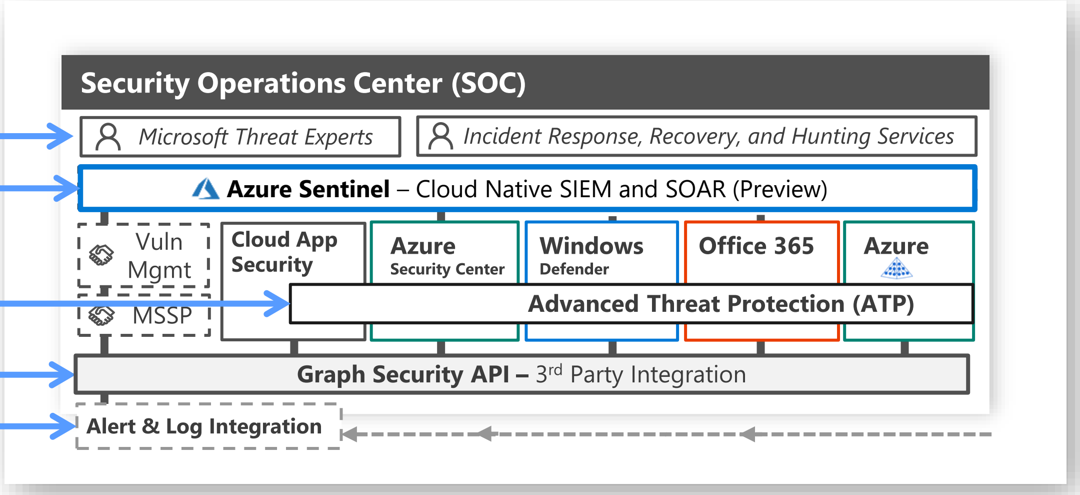
Security Operations Centre (SOC)

Challenges

- Legacy model results in **wasted security expertise**
  - **Analyst Overload** - too many false positives
  - **Poor Investigation Workflow**
  - **Manual integration** for tools and threat intelligence
  - Constantly evaluating products

Microsoft's approach

- ✓ Assist with **Incident Response and Recovery** as well as proactively **hunting for adversaries**
- ✓ Cloud-native SIEM+SOAR for simplifying advanced detection, investigation, and remediation
- ✓ **Integrated investigation experience** across all assets include deep visibility into Windows/Linux/ Mac desktops and servers, Office 365, Active Directory, and Azure Tenants.
- ✓ **Integrate existing SOC tools** and Microsoft capabilities with **Graph Security API** and Log Integration
- ✓ Intelligent Security Graph provides **integrated intelligence** for detection



Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, and Hunting Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Windows Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Intelligent Security Graph

About risual

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

We deliver in partnership with our clients, through the principles of co-working, co-design and co-delivery.

Microsoft Gold Partner across 15 categories and an Azure Expert MSP, placing us in the top 0.05% of MS partners globally.

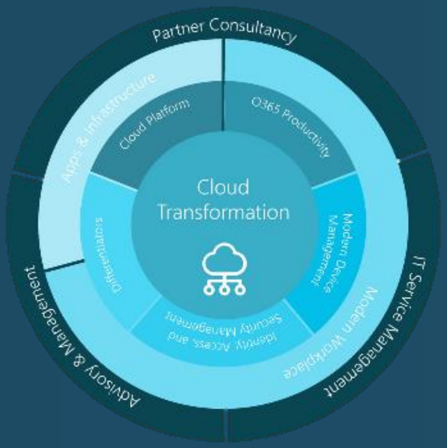
15+ years transforming the workforce through the introduction, adoption and strategic management of Microsoft cloud technologies.

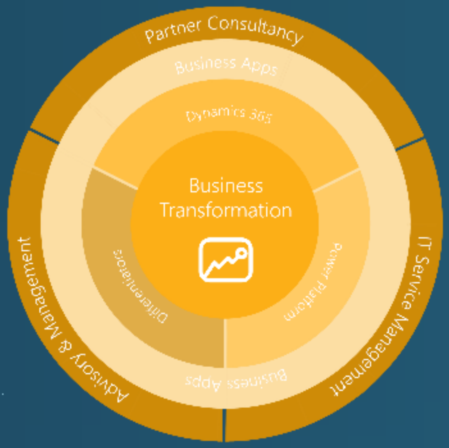
We have Microsoft advanced specialisations in Change and Adoption and Calling for Microsoft Teams validating our extensive capabilities in these solution areas.

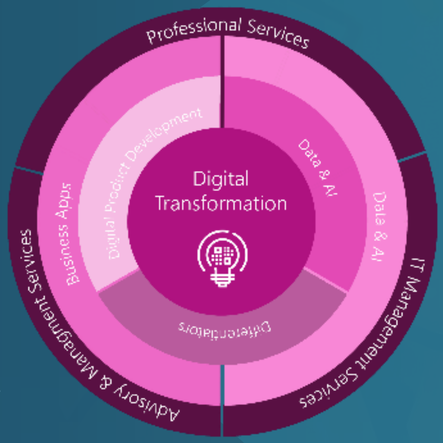
We're driven by a real purpose to introduce sustainable change and drive positive social impact, by increasing the opportunities available to young and disadvantaged people.

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 Work 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

Cloud Transformation Services

For the past 15 years we've worked with clients to transform the workplace/workforce with the introduction, adoption and strategic management of Microsoft cloud technologies. Working across all industry sectors, we aim to transform the ways in which people work and organisations deliver services, through the re-imagination of technology and support services, and through the provision of enhanced digital skills training and apprenticeships.

Cloud Platform

We are experts in the configuration and migration of services & applications to the Cloud. We share our skills and experience as an Azure Expert MSP, leveraging our deep Microsoft relationship to deliver innovative solutions that solve real business problems through a range of services covering the entire Azure ecosystem.

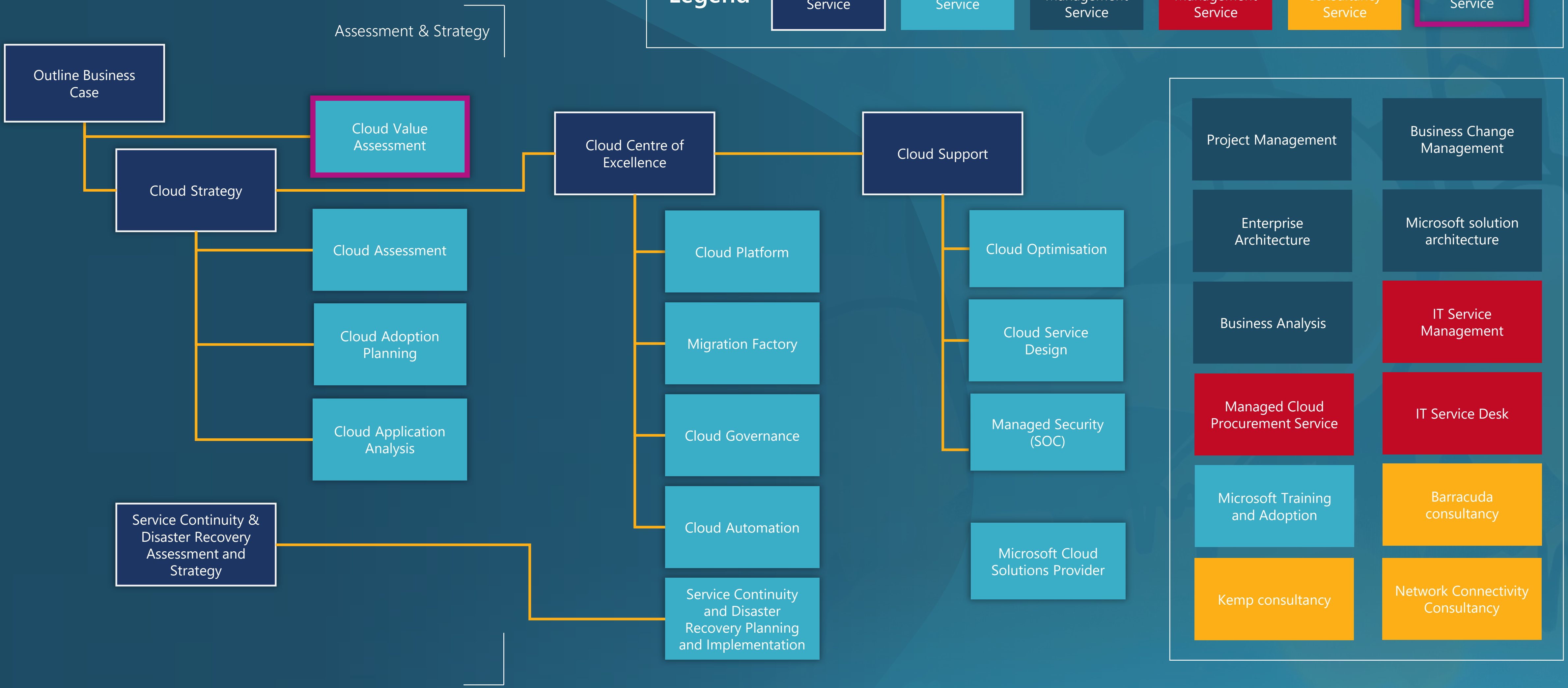
Modern Work

We help our clients get the most from their investments in Microsoft 365 through correct licensing, configuration, training and adoption. We take a user-centric approach, shifting attention to connecting people and giving them the tools and knowledge needed to become a truly Modern Workforce.

Cloud Platform

Legend

- Strategy Service
- Tactical Service
- Advisory Management Service
- IT Service Management Service
- Partner consultancy Service
- Unique risual Service



Assessment & Strategy

- Outline Business Case
- Cloud Value Assessment
- Cloud Strategy
  - Cloud Assessment
  - Cloud Adoption Planning
  - Cloud Application Analysis
- Service Continuity & Disaster Recovery Assessment and Strategy

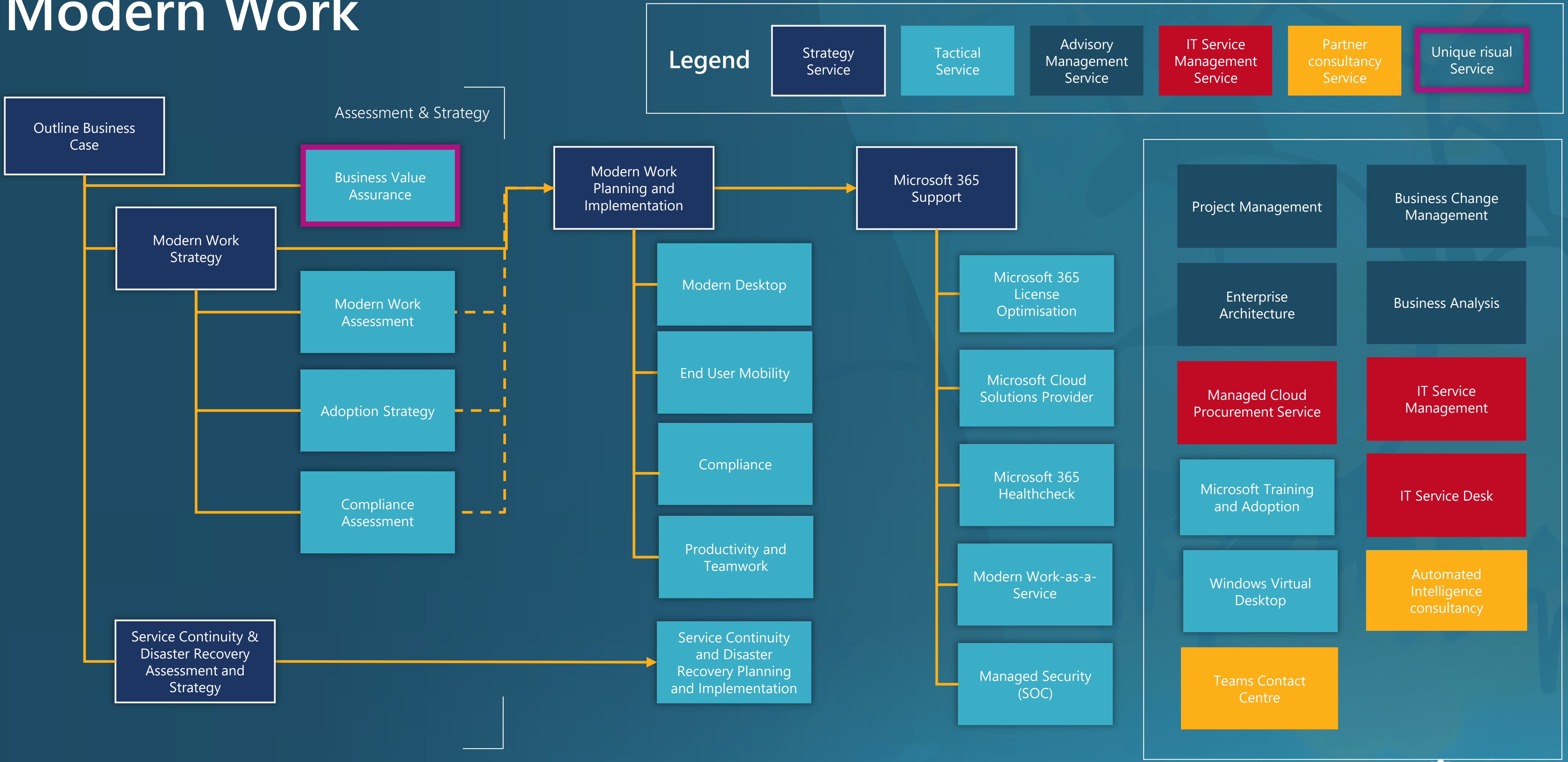
- Cloud Centre of Excellence
  - Cloud Platform
  - Migration Factory
  - Cloud Governance
  - Cloud Automation
  - Service Continuity and Disaster Recovery Planning and Implementation

- Cloud Support
  - Cloud Optimisation
  - Cloud Service Design
  - Managed Security (SOC)
- Microsoft Cloud Solutions Provider

- Project Management
- Business Change Management
- Enterprise Architecture
- Microsoft solution architecture
- Business Analysis
- IT Service Management
- Managed Cloud Procurement Service
- IT Service Desk
- Microsoft Training and Adoption
- Barracuda consultancy
- Kemp consultancy
- Network Connectivity Consultancy

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

Modern Work



Legend

- Strategy Service
- Tactical Service
- Advisory Management Service
- IT Service Management Service
- Partner consultancy Service
- Unique risual Service

Assessment & Strategy

- Outline Business Case
- Business Value Assurance
- Modern Work Strategy
- Modern Work Assessment
- Adoption Strategy
- Compliance Assessment
- Service Continuity & Disaster Recovery Assessment and Strategy

Modern Work Planning and Implementation

- Modern Desktop
- End User Mobility
- Compliance
- Productivity and Teamwork

Service Continuity and Disaster Recovery Planning and Implementation

Microsoft 365 Support

- Microsoft 365 License Optimisation
- Microsoft Cloud Solutions Provider
- Microsoft 365 Healthcheck
- Modern Work-as-a-Service
- Managed Security (SOC)

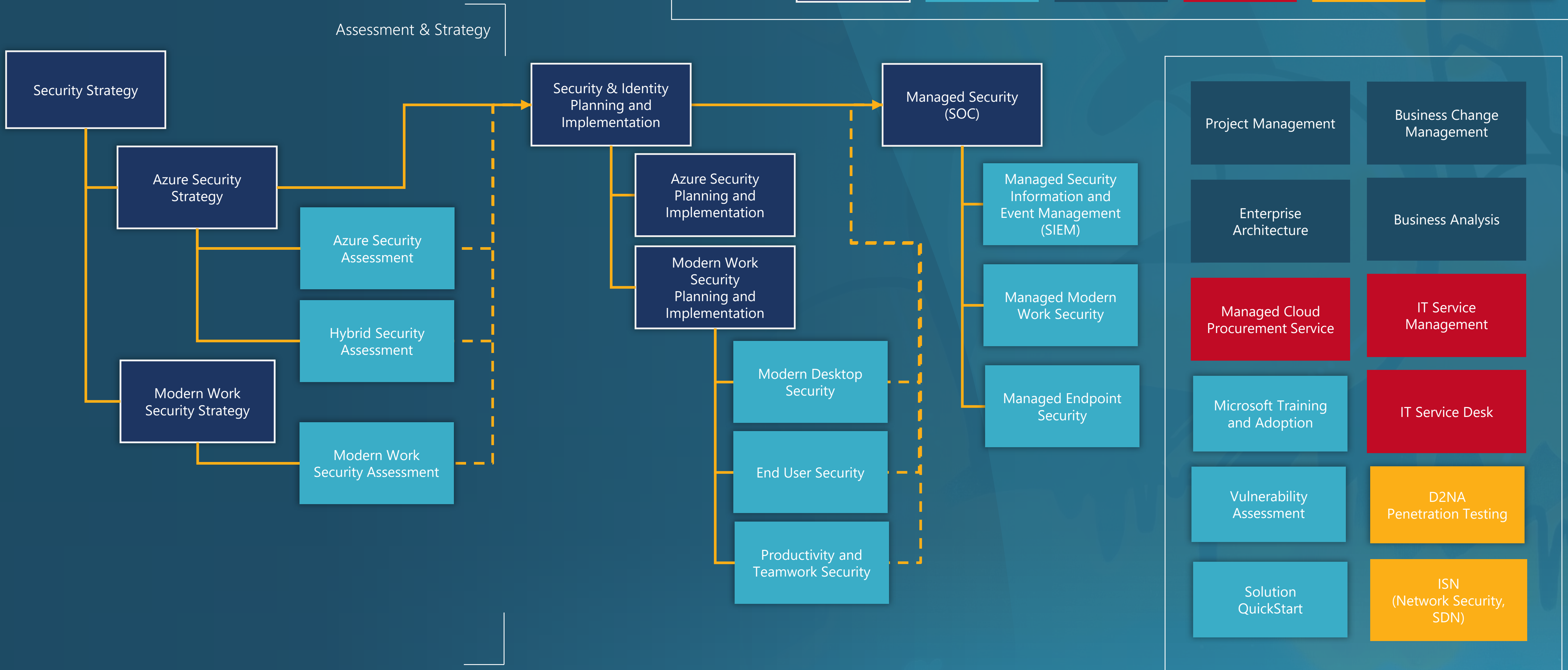
- Project Management
- Business Change Management
- Enterprise Architecture
- Business Analysis
- Managed Cloud Procurement Service
- IT Service Management
- Microsoft Training and Adoption
- IT Service Desk
- Windows Virtual Desktop
- Automated Intelligence consultancy
- Teams Contact Centre

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

Microsoft Security & Identity

Legend

Strategy Service	Tactical Service	Advisory Management Service	IT Service Management Service	Partner consultancy Service	Unique risual Service



Assessment & Strategy

Security Strategy

Azure Security Strategy

Azure Security Assessment

Hybrid Security Assessment

Modern Work Security Strategy

Modern Work Security Assessment

Security & Identity Planning and Implementation

Azure Security Planning and Implementation

Modern Work Security Planning and Implementation

Modern Desktop Security

End User Security

Productivity and Teamwork Security

Managed Security (SOC)

Managed Security Information and Event Management (SIEM)

Managed Modern Work Security

Managed Endpoint Security

Project Management

Business Change Management

Enterprise Architecture

Business Analysis

Managed Cloud Procurement Service

IT Service Management

Microsoft Training and Adoption

IT Service Desk

Vulnerability Assessment

D2NA Penetration Testing

Solution QuickStart

ISN (Network Security, SDN)

Who we work with

Ministry of Housing,
Communities &
Local Government

Ministry of Housing,
Communities &
Local Government

Partnering with risual

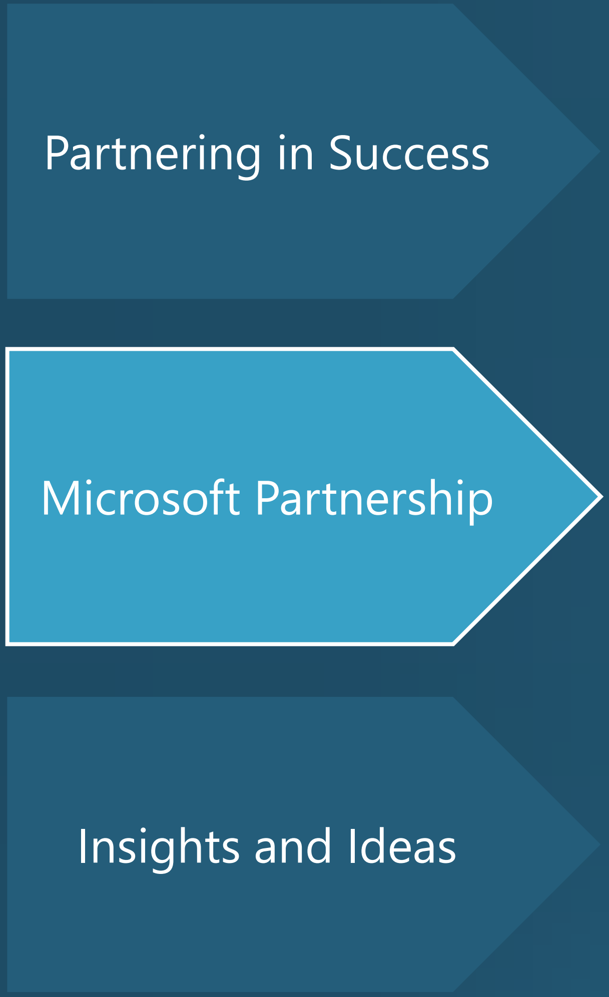
Partnering in Success

Microsoft Partnership

Insights and Ideas

- Fully understand how your service operates, so that we augment and compliment your existing capabilities.
- We will match and mirror your culture to deliver exceptional customer satisfaction.
- Identify and build agility into your systems and processes to help improve efficiencies.
- Drive optimisation and enhance decision making through automation and use of data.
- Provide advice and guidance on the latest trends for people, processes and technology.
- We lead with insight, not solutions, helping you to achieve more value.
- We continually invest in new technologies to optimise costs and help meet increasing customer expectations.

Partnering with risual



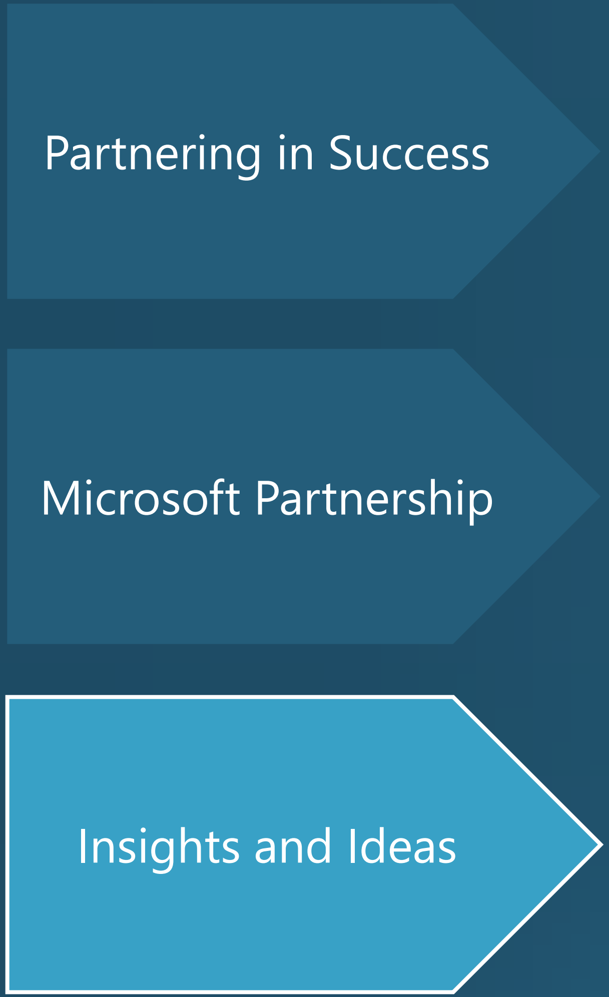
Partnering in Success

Microsoft Partnership

Insights and Ideas

- Eligible funding only available to risual as an Azure Expert MSP, in addition to regular funding from Microsoft.
- Microsoft Fast Track Ready Partner. Can help you get more from cloud productivity services (Office 365).
- Jointly hosted events and seminars with Microsoft thought-leaders and solution architects.
- Microsoft learning and education for staff and technical teams.
- Incentive schemes for both our clients and risual to help drive productivity for your people.
- Microsoft managed partner for Azure, Dynamics 365 and Microsoft 365.
- Engaged in multiple preview programmes across the Microsoft technology spectrum.

Partnering with risual



Partnering in Success

Microsoft Partnership

Insights and Ideas

- Regular webcasts on current and emerging technology.
- Workshop and immersion days to explore use cases for new technology.
- Hackathons – rapid, three-day development cycles to deliver proofs of stake in emerging technology.
- Events with guest speakers from across our client base and technology leaders such as Microsoft.
- Partnership with Gartner for their global industry insight events.
- Active social media campaigns, with blogs, news, insights and client case studies.
- Adoption clinics to help your staff get the most from Microsoft productivity tools.

risual

Experts in Transformation

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