Reliance acsn
Specialists in IT Security Management

SUITS YOU.
SECURITY DEVICE MANAGEMENT

HELPING YOU TO MAINTAIN OPERATIONAL EXCELLENCE

Reliance acsn Security Device Management services provide quality, flexible, responsive, and scalable managed security solutions, for all aspects of your organisation's security infrastructure 24x7x365.

Our expert team are highly accredited and experienced in all core security infrastructure technologies and vendors, and can work hand-in-hand with your existing IT team, or take full responsibility of the management of your security infrastructure.

With several Reliance acsn managed service packages to choose from; we can tailor each service to your business, infrastructure portfolio and requested contract hours.

This means you benefit from the quality derived from the consistency of a packaged service offering, but one that's entirely tailored to your exact business needs and requirements.

Our services are designed to offer flexibility underpinned by a consistent approach and an agreed service level agreement.

- ADDS/MOVES/CHANGES
- ONGOING SERVICE MANAGEMENT
- HEALTH, WELLBEING & CAPACITY MANAGEMENT
- CUSTOMER PORTAL
- MONTHLY REPORTING
- PATCH /UPGRADE MANAGEMENT

RELIANCE ACSN LIMITED
2nd Floor, 3 Valentine Place,
London SE1 8QH

Reliance acsn
Specialists in IT Security Management

T: +44 (0)845 519 2946
E: contact@relianceacsn.co.uk
W: www.relianceacsn.co.uk

HOW WE CAN SUPPORT YOU

Reliance acsn provides a Security Device Management service in one of two ways:

CO-MANAGED | Reliance acsn's Co-Managed Service enables the client to retain management of security devices in-house, but with the added benefit of easy access to expert, highly responsive IT security specialists whenever and wherever you need them.

FULLY-MANAGED | There are, however, situations where maintaining the right number and type of internal security resources can be impractical or not financially viable. Fully-Managed services from Reliance acsn can be tailored to your specific requirements and typically involve Reliance acsn taking complete operational control of the devices under management. Whether they are centrally hosted at Reliance acsn's data-centres, in the cloud, or deployed on-premise at your sites.

Reliance acsn engages with you to determine the service delivery model that is best suited and fit-for-purpose, whether that is as a virtual security team or as an extension to in-house resources, all backed by robust SLA's.

OUR APPROACH
A cyclic process that involves…

REVIEW
The review stage is the project initiation phase. During this stage, Reliance acsn will assign a project manager to the project and go through a process of planning and discovery with you

MANAGE
Where the solution has transitioned to operational mode and where business-as-usual (BAU) monitoring, management and support of the serviced devices takes place. This also includes the implementation of all service level management and ongoing service reviews.

ON BOARDING
The service on-boarding stage is where the implementation of the service takes place, once the initial planning and discovery has been concluded. Reliance acsn will assign a service transition manager who will be responsible for ensuring smooth transition into an operational service

IMPROVE
The final stage of the engagement model is an iterative project phase of service review and improvement conducted in partnership with you and based on the service level management and review tasks taking place in the 'manage' stage

ABOUT RELIANCE ACSN:
We are a Digital and Cybersecurity Service provider and we believe results come from a well-executed and business-integrated approach stemming from the application of our skills and expertise, combined with threat intelligence and effective risk management.

- ACSN was founded in 2003. Reliance acsn was born through merger with Reliance Cyber Science in 2016.

- We have a highly skilled and experienced team, with an ambitious plan underway to grow significantly in the near future.

- We've built strong partnerships with over 80 customers across 5 continents, helping them to address Digital Transformation and Cybersecurity challenges.

- Our staff are accredited by all the major security vendors and are able to support virtually any technology you have in place or you've been planning to procure.