SaaS Security

RWS

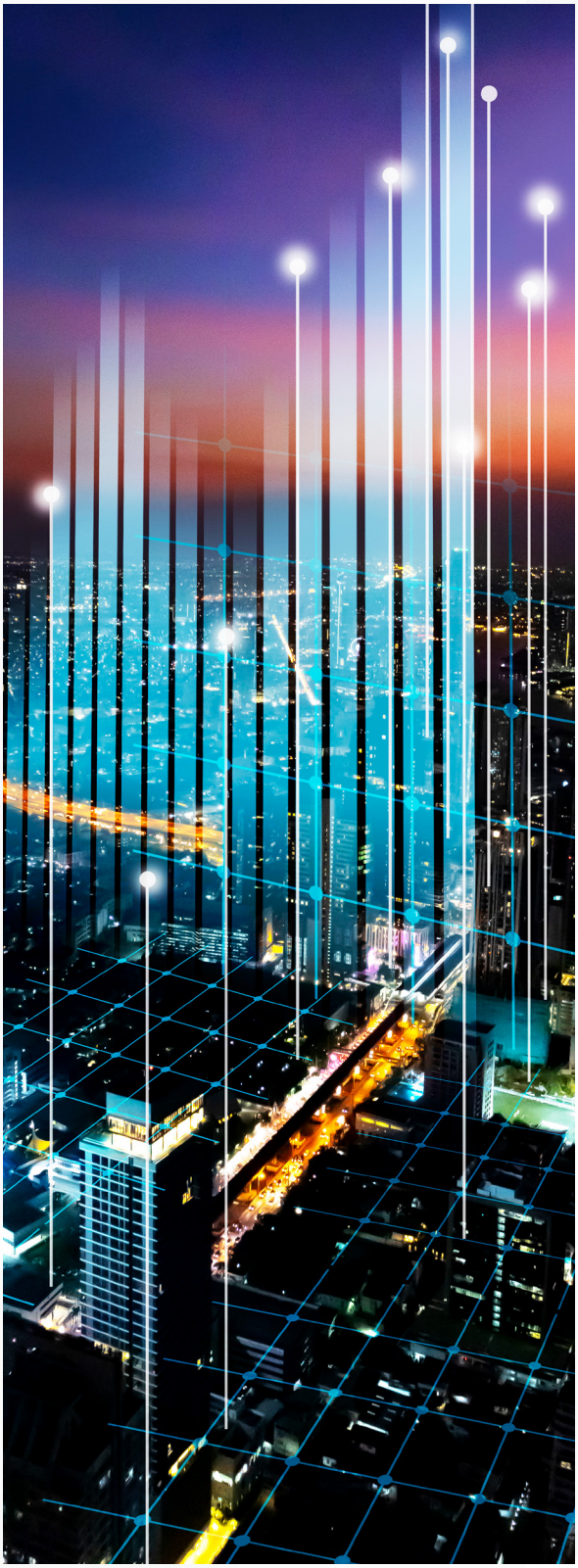
Contents

Introduction

RWS's Software as a Service (SaaS) environment consists of multiple products and capabilities, with services catering to 600-plus global clients, including over 85 Fortune 100 companies. With such a diverse and prominent customer base, RWS's security programme needs to constantly evolve. It must cater to individual verticals of the market and stay finely tuned to ensure these companies have the confidence in outsourcing their data protection and privacy to us.

The protection of our clients' data is paramount to our business and we prioritize keeping their information secure. RWS pledges to protect your business and data with industry-leading security tools that meet the highest levels of compliance with regulations, standards and certifications, including GDPR, ISO-27001, SOC 2 and others. With special attention to regulated markets like the Finance and Life Science sectors, our cloud services are tailored to provide a modern, multi-tiered security programme, maintain high availability and ensure quick recovery in the event of a disruption.

This overview details how RWS manages security in day-to-day operations, including system administration, business continuity management, security and operations, data centres and privacy.



Cloud service providers

RWS has contracted with the following top-tier, leading third-party service providers to host RWS products:

Amazon Web Services (AWS)

RWS partners with Amazon Web Services (AWS) to provide hosted deployment of RWS products. AWS maintains multiple certifications for security, the most relevant of which are ISO-27001, CSA STAR and SSAE16 SOC 1, SOC 2 and SOC 3.

Alibaba Cloud

RWS also partners with Alibaba Cloud to provide hosted deployment of RWS products. Alibaba cloud maintains multiple certifications for security, the most relevant of which are ISO-27001, ISO-27017, CSA STAR and SSAE16 SOC 1, 2 and 3.

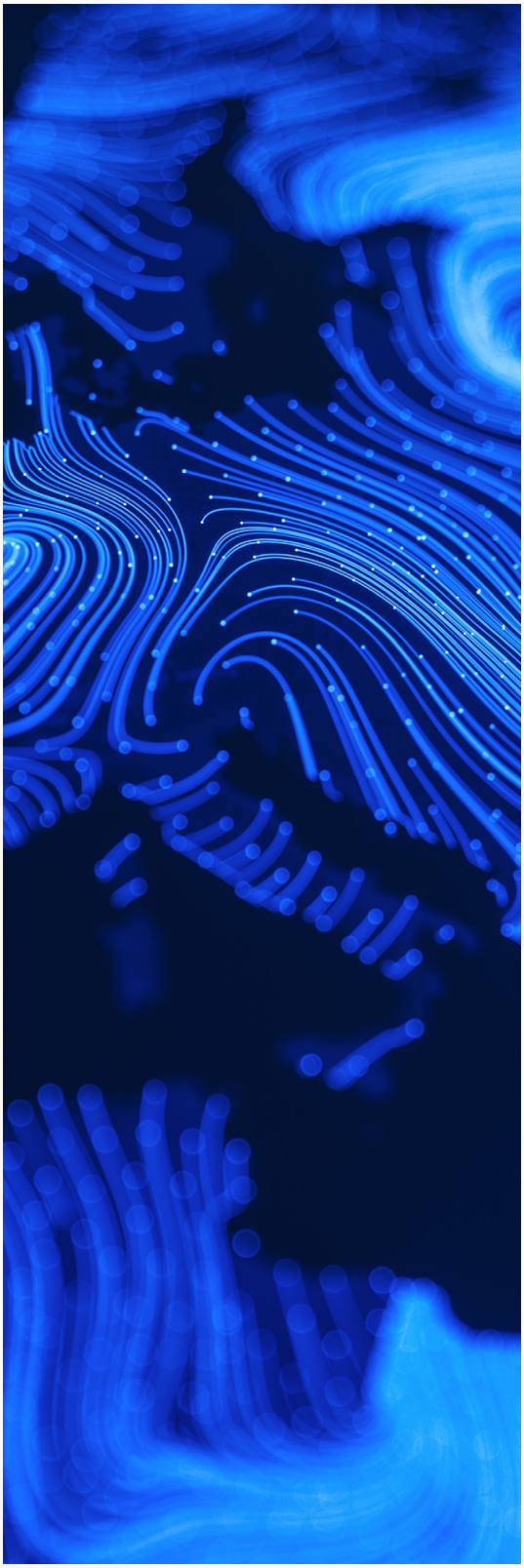
Identity and access management (IAM)

Multifactor authentication (MFA) is enabled for the management of all cloud service provider infrastructure. Only authorized personnel have access to the cloud service providers' management consoles and tools. All actions in the management console and tools are logged and stored centrally. Monitoring and review of these logs occurs continuously based on standard operating procedures. RWS has a comprehensive hybrid cloud security framework for access controls, accountability, authorization and governance for any action undertaken by our personnel. Comprehensive security log aggregation and industry-leading tools ensure compliance and help identify threats. RWS has access control policies in place that apply to all operational personnel. Access is granted on an as-needed basis, following the principle of least privilege, and is reviewed periodically.

RWS collects, aggregates, indexes and analyzes access control log data to detect intrusions, threats and behavioural anomalies. As cyber threats become increasingly sophisticated, real-time monitoring and security analysis is required for rapid threat detection and remediation. Our highly-trained security experts use an advanced set of tooling to provide security intelligence and monitoring and response capabilities, and to perform data analysis on access audit logs.

RWS's standard service locations around the world

RWS deploys SaaS Services for our customers around the globe. Hosting regions are selected to meet customer data residency and related requirements, while enabling redundancy and recovery in the event of a regional incident. For available locations, please see the Service Catalogue for the specific SaaS service.



Availability and proactive monitoring

RWS uses a variety of tools to proactively monitor responsiveness and availability of SaaS Services. Alerts are managed by RWS's Cloud Operations Center, which is staffed 24x7x365. Application deployments and infrastructure are continually scanned for vulnerabilities and patched to protect against new exploits and ensure the highest possible security, be that at the operating system level, the application level or anywhere else in the technology stack. RWS uses automated measures to ensure underlying infrastructure is up to date with the latest system and security patches. RWS's R&D constantly scans their software products, including third-party dependencies, to ensure any vulnerabilities are patched with urgency. Redundant external connectivity, advanced mitigation and routing techniques and a specific, managed Distributed Denial of Service (DDoS) tool are used for protection against sophisticated DDoS attacks.

Physical protection

The applications and services offered by RWS are hosted in multiple public clouds and are protected against various threats by the respective cloud service providers. Access is scrutinized and entry is controlled and monitored. The perimeter layer includes a number of physical security features which can, depending on the location, include security guards, fencing, security camera feeds, intrusion detection technology and other security measures.

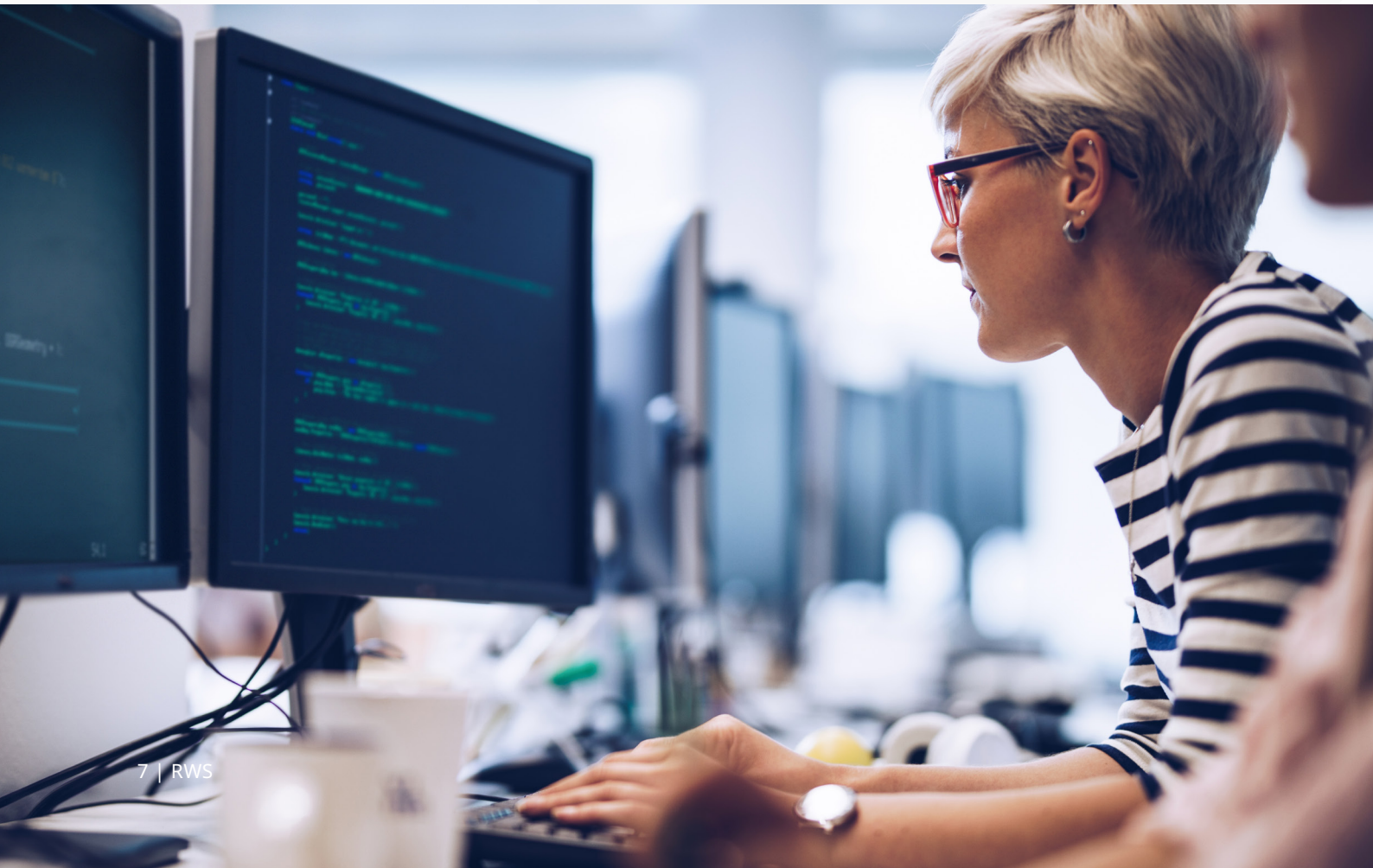
Data security and logical protection

Logical security measures are also implemented, with RWS's SaaS services running and managed by a dedicated Cloud Operations team, separate from RWS's corporate systems. Customer data is always logically segmented, and both live and backup data are encrypted at rest. Access to systems, data and backups is limited to only those staff who need access to perform their job duties. It is governed according to the principle of least privilege, by staff who have received role-based, security-minded training and have undergone background checks based on local regulations. Backups are taken daily and are retained for up to four weeks to ensure point-in-time recovery. Networks are segmented so only servers whose role requires access from the internet are in the demilitarized zone (DMZ). All internet traffic is passed through a firewall and gateway, decreasing the footprint for attacks and increasing detection possibilities.

Business continuity and disaster recovery

RWS's SaaS strategy focuses on deploying services and retaining backups in multiple data centers and regions (where available), protecting RWS and its customers from catastrophic failures due to natural disasters and major disruptions impacting individual locations. Locations are selected to provide redundancy while still meeting agreed-upon customer requirements for data residency.

RWS Cloud Operations staff are globally distributed to protect against a regional incident impacting the management of SaaS Services and ensure 24x7x365 service.



Certification and compliance

Hundreds of enterprise customers entrust their data to RWS's SaaS services every day and RWS aligns its operations to industry-leading standards and certifications, as well as relevant regional regulations. These include:

GDPR

ISO 9001:2015 (Quality Management Systems)

ISO 27001:2013 (Information Security Management Systems)

SOC 2, Type 2

ISO 21500:2012 (Project Management)

In support of these certifications and regulatory compliance, RWS maintains a robust set of policies. Information on these policies and an FAQ are available from rws.com/legal/security. The policies themselves are classified RWS internal-only.

All new RWS staff receive training on these policies, as well as staff Information Security responsibilities. Existing staff receive annual refresher training.

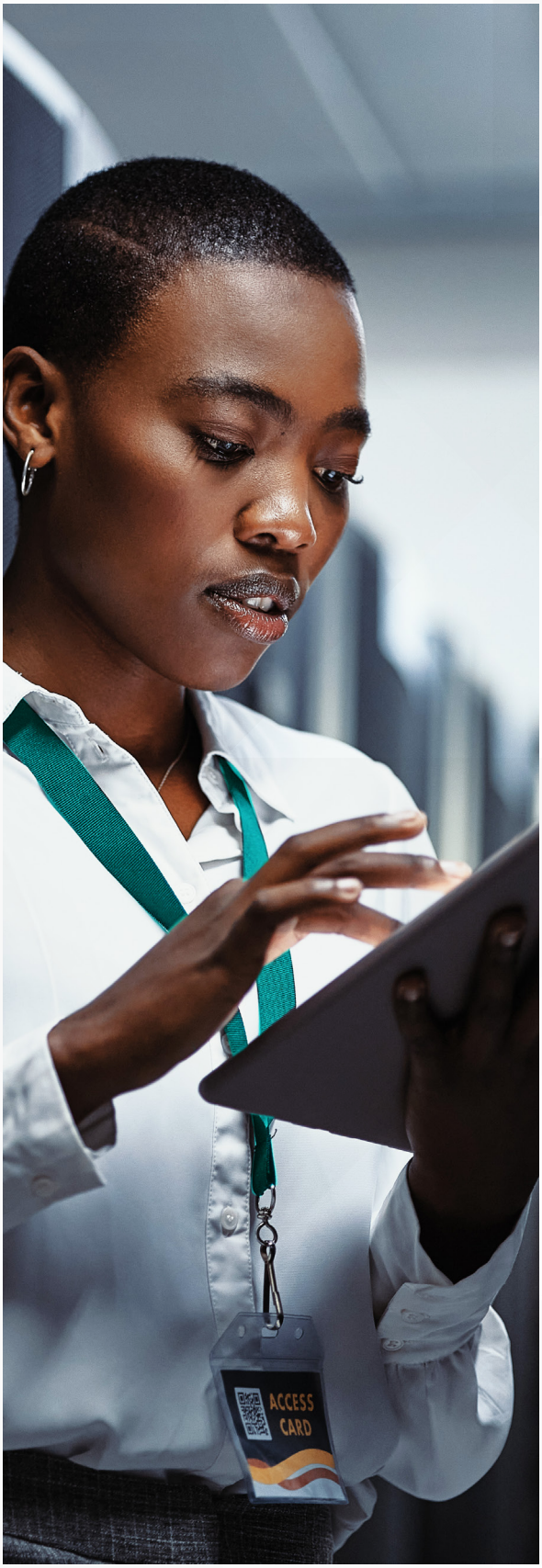
RWS also ensures any sub-processors meet or exceed the certifications and compliance that RWS maintains.

We are continually evaluating further certification and compliance requirements.

Risk assessment

RWS has documented a comprehensive risk assessment plan consistent with the ISO 27001:2013 standard.

All risks are documented in a Risk Register. The RWS Security and Compliance team host a recurring review of all open risks within the Risk Register and add any new risks deemed relevant to the estate. This process involves key stakeholders from the business and will include a review of the likeliness and impact of risks, remediation plans (treatment plan) and potential mitigations. RWS Cloud Operations Managers perform risk assessment for their respective processes with the assistance of the RWS Cloud Security Operations team. These teams are responsible for regularly reviewing the risk management framework to assess, analyze and manage risks to the lowest acceptable level for the system environment and effectiveness of controls.



RWS security tools capabilities

- RWS uses industry-leading security software for security information and event management (SIEM) including log consolidation and analysis, and file integrity monitoring.
- RWS has implemented perimeter firewalls, intrusion detection and prevention services, endpoint protection (anti-malware) and extended detection and response (XDR) tools to monitor network traffic, data, and logs, enabling the detection and prevention of malware infestations, breaches and intrusions. Modules are automatically updated with signatures from vendors as soon as they are released.
- The Cloud Operations Center team operates 24x7x365 to support real-time event management activities.
- RWS uses industry-recommended tools for threat visibility and ensures compliance of our cloud footprint by combining threat detection, predictive analytics, security configuration management and automated incident response.
- All systems are deployed according to a system hardening profile that adheres to Centre for Information Security (CIS) guidelines.
- RWS has configured an industry-leading vulnerability scanning tool to conduct regular automated scans on its infrastructure and deployed services, including OWASP top 10 compliance and reporting.
- Penetration testing is done against all new major versions of products, or every 12 months.
- RWS uses an IT Infrastructure Library (ITIL)-compliant ticketing tool for incident management (including security incident management), request fulfilment, service level management, problem management and change management.
- RWS uses extended detection and response (XDR) tooling to proactively identify potential threats and quickly respond.
- The security team is part of the Change Advisory Board (CAB) to review all changes from a security perspective.

In summary, RWS provides the most extensive security operations suitable for highly regulated industries, while continuing to evolve our security offerings to address new threats, regulations and requirements.

For more information about our approach to security

rws.com/legal/security

About RWS

RWS Holdings plc is a unique, world-leading provider of technology-enabled language, content and intellectual property services. Through content transformation and multilingual data analysis, our unique combination of technology and cultural expertise helps our clients to grow by ensuring they are understood anywhere, in any language.

Our purpose is unlocking global understanding. By combining cultural understanding, client understanding and technical understanding, our services and technology assist our clients to acquire and retain customers, deliver engaging user experiences, maintain compliance and gain actionable insights into their data and content.

We work with over 80% of the world's top 100 brands, more than three-quarters of Fortune's 20 'Most Admired Companies' and almost all of the top pharmaceutical companies, investment banks, law firms and patent filers. Our client base spans Europe, Asia Pacific and North and South America. Our 65+ global locations across five continents service clients in the automotive, chemical, financial, legal, medical, pharmaceutical, technology and telecommunications sectors.

Founded in 1958, RWS is headquartered in the UK and publicly listed on AIM, the London Stock Exchange regulated market (RWS.L).

For further information, please visit: **www.rws.com**