NIS2 and RealVNC Connect

Version 0.1

23rd January 2025

Contents

CSA Cyber

This white paper has been produced in partnership with CSA Cyber who have hands on experience helping organisations achieve compliance across a range of international cyber and information security standards and certifications. CSA Cyber provides cyber consultancy and cyber managed services which help to detect, protect and educate against the ever-changing cyber threat.

CSA Cyber hold the NIS2 Lead Implementer badge showing a key understanding of what is required under the regulations and how organisations can best comply. Alongside being a NIS2 lead implementor, CSA Cyber are also ISO27001 lead implementors and lead auditors which is crucial with NIS2 and ISO27001 being so closely aligned.

What is NIS2

The Network and Information Security Directive, more commonly known as NIS2, is the updated EU directive replacing the original NIS Directive. This EU directive specifies cybersecurity requirements that need to be implemented by EU companies that are considered critical infrastructure, with member states specifying the minimum levels of cybersecurity that organizations must achieve.

It is estimated that 100,000 organizations will have to become NIS2 compliant with strict penalties in place for those who do not reach the specified level of compliance. With RealVNC Connect, your organisation will receive the business benefits of remote access software without jeopardizing NIS2 compliance.

This document has been structured to detail how both RealVNC as a business and how the use of RealVNC Connect remote access services can support organizations with their NIS2 Compliance.

Note: The information contained in this document is not legally binding, nor do we intend for it to be used as legal advice. Instead, we recommend providing your auditor or compliance team with a copy of this document to help you NIS2 audit go as smoothly as possible.

What guidelines must remote access software follow?

NIS2 encompasses a wide range of controls that organizations must understand and ensure are implemented in order to remain compliant, these are:

Article	Title
20	Governance
21	Cybersecurity risk-management measures
22	Union level coordinated security risk assessments of critical supply chains
23	Reporting obligations
24 & 25	Use of European cybersecurity certification schemes & Standardisation

Although NIS2 does not mandate ISO27001 implementation, it does reference the ISO/IEC 27000 series in its preamble as a means of instituting cybersecurity risk management. Moreover, NIS2 actively promotes the adoption of international standards making sure organizations view cybersecurity holistically adopting a range of standards to cover key aspects needed for a strong security posture.

By being certified under ISO27001, RealVNC are already aligned to key guidelines under these 6 articles showing a high level of compliance following the NIS2 guidance.

Key terminology

Throughout this document, we refer to certain RealVNC-specific terminology.

RealVNC Connect is remote access software consisting of two apps: VNC Server and VNC Viewer. You must install and license VNC Server on the computer you want to control. This is known as your VNC Server computer.

You must then install VNC Viewer on the computer or device you want to take control from, which is known as your VNC Viewer device. You do not need to license this device, meaning you can freely connect to your VNC Server computer from as many devices as you wish.

Note on RealVNC Connects cloud connectivity

RealVNC Connect offers the ability to make remote access connections via RealVNC-managed cloud services (‘cloud connections’). This data is end-to-end encrypted in such a way that RealVNC has no means to decrypt or read it, technical or otherwise. Critically, RealVNC’s only interaction with this encrypted data is to transfer it. When a direct connection is used for on-prem deployment however, RealVNC online services will not be used at all.

For cloud-brokered connections, RealVNC acts as a conduit of information and is a transport-only service. As such, as per the FAQ listed, RealVNC is not considered a ‘business associate’, and no Business Associate Agreement is required.

RealVNC Connect also allows for direct connectivity. For the avoidance of doubt, no cloud services are involved for connections made directly via UDP or TCP. For more information, see our document on cloud vs direct[1].

[1]Cloud vs Direct- https://help.realvnc.com/hc/en-us/articles/360024750892-What-are-cloud-connections-and-direct-connections

How does RealVNC and RealVNC Connect support NIS2 regulations?

The NIS2 regulations dictate a range of mandatory controls that must be followed. This paper has split these controls down into key titles alongside how RealVNC comply showing organisational risk management and security controls are in line with NIS2.

Each EU country will be transposing its own cybersecurity laws based on the NIS2 directive, which has specified the minimum level of cybersecurity which companies will have to achieve

Please see the overview table below which outlines how RealVNC looks to implement and follow the key requirements of NIS2 as well as helping customers follow NIS2 requirements surrounding their own critical and important supply chain obligations. For a comprehensive analysis, please refer to the detailed analysis of how RealVNC and RealVNC Connect can help your organisation in the compliance of NIS2.

Key NIS2 Requirements	**RealVNC Response**
Governance structure which supports senior management understanding and implementing security controls.	- RealVNC ensure that risk management is a key activity for senior management alongside an accountable figure who sits on the board. - Through dedicated training and incident management activities, RealVNC understand risk management should involve all levels of the organisation allowing for a holistic and constantly evolving understanding of risks associated with the organisation as well as those for customers. - RealVNC are aligned to ISO27001 showing a mature governance regime is in place which understands risk management and the necessary requirements to manage information security.
Use of risk assessments alongside effective security policies and procedures.	- A mature policy and procedure suite supports the RealVNC governance regime covering NIS2 risk management requirements. - These allow for the protection of network and information systems alongside specific requirements such as encryption, HR security and the development and maintenance of systems, ensuring RealVNC solutions are secure and remain operational.
Business continuity and disaster recovery plans in place and regularly updated.	- A tested and annually updated Business Continuity and Disaster Recovery plan is in place to support a high level of organisational resilience allowing RealVNC solutions to maintain specified uptime requirements. - RealVNC Connect provides customer support for their own Business Continuity and Disaster Response activities.
Security in place for the procurement, development and / or operation of systems.	- Within the RealVNC policy and procedure suite, dedicated security procedures are in place for the creation and development of software relied upon by customers to support their own critical business functions.

The presence of up-to-date cyber security training.	- Annual cyber security training is in place across the organisation to support current cyber hygiene best practises. - Added training requirements are in place for those in specialist or senior roles to maintain operational resilience at the top of the organisation.
The effective use of multi factor authentication.	- Current best practice MFA is in place across RealVNC ensuring the protection of data. - RealVNC Connect supports various MFA solutions ensuring customers compliance with key NIS2 requirements when using third party software within their own IT architecture.
Supply chain security.	- Supply chain risks associated with RealVNC have been mapped with key mitigations in place alongside mature policies and procedures. - Supply chain risks are regularly reviewed to maintain an understanding of any developments associated with the risk profile of RealVNC and their customers.
Understanding of reporting guidelines.	- RealVNC understands the importance of reporting obligations required under NIS2 and can support customers through dedicated SLAs. - Please see Table 1 for more information.

Governance

RealVNC

1. RealVNC ensure there is a mature governance regime which encapsulates Article 20 of the NIS2 regulations.
    a. As a part of this governance regime, cybersecurity training is completed annually across the organisation ensuring all employees at RealVNC understand current threat landscape and the associated cyber security risks, how best to identify and subsequently mitigate them.
2. Management is aware of the cybersecurity measures in place and oversee, approve and are appropriately trained to make decisions that ensure a board level understanding of cyber risks.
    a. There is an accountable figure at board level who oversees Cyber and Information risk management.
    b. Regular high-level training such as tabletop exercises are conducted which involves management to understand the most up to date risks to RealVNC.

RealVNC Connect

1. RealVNC Connect supports an organizations governance regime by improving oversight and accountability enabling real time monitoring and logging improving transparency.
    a. The use of audit logging allows customers to view key events such as user role changes or when cloud connections are made to a specific device.
    b. By default, logging is in place for all basic connection activity and is automatically enabled to event logs or syslog dependant on the operating system in place.
2. Centralised management within RealVNC Connect allows controls to enhance governance supporting and enforcing policies in place while also effectively controlling user permissions.

Risk Management

RealVNC

1. Cybersecurity risk management
    a. RealVNC have a mature and up to date policy suite which encompasses the protection of information systems, the physical environment and network protection. These are available for review on request from our trust centre[2] and include:
        i. Risk Management Policy
        ii. IT Security Policy
        iii. Business Continuity Plan & Incident Response Plan
        iv. Backup Policy
        v. Supplier Management Policy

[2] RealVNC Trust Centre - https://trust.realvnc.com

vi. Software Development Lifecyle (SDLC)
vii. Access Control Policy
viii. Acceptable Use Policy
ix. HR Security Policy / HR for Contractors Policy
x. Cryptography Policy
xi. Network Security Policy
xii. Audit Policy

b. Cyber Resilience for RealVNC
    i. Monthly vulnerability scans are completed alongside annual penetration tests ensuring a secure and resilient environment across the organisation.
c. The use of multi-factor authentication is in place across RealVNC internal IT infrastructure supporting current high level security guidelines.
    i. Supporting high level MFA practices shows RealVNC align their practices with NIS2.
d. Encryption practices
    i. Where encryption is necessary, strong cryptography and key management processes and procedures are implemented.
e. Network security information
    i. Management of wireless networks with appropriate safeguards in place.
    ii. Network segregation in place between RealVNC and RealVNC Connect Infrastructure.
    iii. Firewalls in place as a barrier to external traffic.
    iv. Monitoring of the network alongside pre-agreed KPIs.
    v. Annual CREST certified penetration testing.
    vi. Geographically diverse infrastructure with no single points of failure.
f. Supply chain management
    i. Initial due diligence checks evaluating third party data processors, including but not limited to:
        (i) Encryption baseline
        (ii) GDPR conformity
        (iii) Evaluation of cloud services
        (iv) Various code of conduct conformity
    ii. Annual monitoring of third parties after gaining approval.

RealVNC Connect

1. Cybersecurity risk management
    a. RealVNC Connect has been developed in line with RealVNC policies and procedures alongside a proactive SDLC policy.
    b. Authentication is in place for RealVNC Connect as a secure solution
        i. Accounts are secured using email-based 2FA by default.
        ii. RealVNC Connect supports various means of MFA including;
            (i) VNC Password
            (ii) System Authentication
            (iii) Interactive System Authentication
            (iv) Single Sign On (Kerberos)

(v) Smartcard/certificate (Yubikey)
(vi) System Authentication (RADIUS and Duo)

iii. System administrators can use their RealVNC account to control which members of a team can discover which computers. If a user is unable to discover a computer, they cannot connect to it.

c. Secure production
   i. In order to provide a secure product, only authorised personnel have access to the production and maintenance of RealVNC Connect.
   ii. Access to production is also monitored ensuring quality assurance throughout alongside ensuring risk management practises are followed and with a high level of transparency throughout the development and maintenance.
   iii. RealVNC employ external security consultants to perform a white box audit on product source code in order to maintain secure development practices.
d. Encryption practices
   i. All connections are protected by 128-bit or 256-bit AES-GCM encryption, depending on your settings and subscription type.
   ii. All connections have perfect forward secrecy, ensuring a high level of protection from the risk of being decrypted
   iii. Online access to your RealVNC account is protected by mandatory TLS. This best practices for secure web development, and our website has an A rating from the Qualys SSL Labs test.
e. Network security information
   i. RealVNC's internal IT networks are physically and logically segregated from product service infrastructure.
   Separate development/test, staging and production environments exist.
   Developers have no access to production.
   Network segregation in place between RealVNC internal IT systems as well as RealVNC Connect product infrastructure.
   ii. System administrators can configure the VNC Server app to determine who has permissions to connect.
   iii. VNC Server is configured by default to identify users according to their unique system account name (e.g. Windows, macOS or Linux account name)
f. Secure Development
   i. In order to ensure the availability of RealVNC Connect, a mature Secure Development Life Cycle process is in place employing the 'shift left' methodology ensuring security at all stages. This limits vulnerabilities that might be present during each phase of development alongside appropriate threat modelling.
   ii. A mature SDLC policy in place which specifies obligation on any outsourced development for RealVNC Connect including sufficient testing, due diligence checks and the signing of confidentiality clauses.

Supply Chain Risks

RealVNC

1. In order to support the Union level coordinated risk assessments of critical supply chains, RealVNC follow stringent supply chain risk management practises to mitigate any risks associated with the supply chain.
    a. RealVNC perform due diligence as part of the supply chain management process, appropriate security clauses are included in contracts and screening checks are performed on any third-party providing services as part of the RealVNC connect infrastructure.
    b. The security controls in place across the RealVNC Connect architecture means that clients can be assured that potential risks to the supply chain have been mitigated.

RealVNC Connect

1. RealVNC ensures that Software Composition Analysis (SCA) tools are in place if third party software is used for development purposes. This ensure the licence type is permitted as well as checking the software does not contain any known vulnerabilities. In addition to provide transparency, Software Bills of Material (SBOM) can be provided on request.

Reporting Obligations

RealVNC

1. RealVNC have specific reporting requirements in place if an incident was to take place which is outlined within a specific Incident Response Plan.
2. RealVNC understands and follows NIS2 requirements ensuring that essential and important entities can notify the relevant authorities in case of a cyber event without undue delay. Please refer to Table 1 for a more detailed look at the reporting obligations organizations must follow.

RealVNC Connect

1. If necessary, there is the option of personalising reporting obligations within specific SLA agreements to be in line with geographic variations which might be included by the relevant national competent authority.
2. RealVNC Connect allows for session logging and auditing meaning remote access activity can be tracked and monitored – and ingested into a SIEM, if required - aiding with any reporting obligations both in a crisis following NIS2 guidelines as well as for more general auditing purposes.

Certification and Standardisation

RealVNC

1. RealVNC are UKAS accredited IS27001:2013 certified showing a high level and mature organisational posture aligned to a recognised international security standard focused on network and information security.
2. RealVNC are also Cyber Essentials certified showing an understanding of baseline security functions aligned to current best practices.

RealVNC Connect

1. Being ISO27001:2013 certified shows that correct procedural practices are in place to support secure development and maintenance of RealVNC Connect. It also shows that information security and data protection is an essential function across RealVNC providing customers with assurance that RealVNC Connect is aligned to these practices.

Business Continuity

RealVNC

1. RealVNC can help organisations with the task of meeting NIS2 obligations for organisations to have effective Business Continuity and Disaster Recovery plans in place.
    a. RealVNC solutions allow organisations to continue operations to provide remote access across the organisation supporting business continuity practices.
    b. RealVNC solutions uptime shows that its products can be relied upon to support disaster recovery activities as well as business continuity practises.
2. Business continuity and Disaster Recovery plans are in place across RealVNC
    a. Regularly reviewed, audited (internally and externally) and tested business continuity and disaster response processes are within the RealVNC Information Security Management System in order to allow the business to return to business as usual in case of a Cyber event or major incident.

RealVNC Connect

1. RealVNC Connect enhances business continuity required under NIS2 allowing an organisation to access business operations without having to be physically on site.
2. RealVNC Connect can be deployed behind an organizations internal firewall on an internal network without requiring devices to have an internet connection, further enhancing its ability to be used for disaster response and business continuity.

How does RealVNC help your organisation to comply with NIS2?

RealVNC's remote access solution is designed to meet and assist with a broad range of industry and government standards and regulations. With remote working becoming a normal practice globally, the risk of accessing data insecurely poses a risk to organizations. This means using a supplier which follows NIS2 standards to the highest level is crucial.

RealVNC's commitment to following the guidelines set within NIS2 of being a secure supplier who takes risk management as a centralised principle allows customers to have confidence that employing remote access solutions does not increase the risk landscape while improving collaboration and enhancing productivity. RealVNC follows and adheres to a range of high-level security principles with the ability to provide evidence to show competent authorities that RealVNC follows its supplier obligations to those both categorised as 'important' and 'critical' under NIS2 guidelines.

By employing secure remote access solutions provided by RealVNC, competent authorities across Europe are shown that your organisation is supporting a mature security posture.

How can RealVNC Connect help your organisation to comply with NIS2?

Using RealVNC Connect can help in your organisation's requirements in following NIS2, which falls under the taking of appropriate and proportionate technical measures related to the ability to report and handle incidents. This is a requirement within Article 21 to manage risks posed to the security of network and information systems as well as preventing and minimizing the impact of incidents through the help of remote access tools.

By using RealVNC Connect, information that is safeguarded can be remotely accessed meaning critical files can be accessed instantly. This is important under NIS2 when referring to business continuity. Organizations are also aiding in preventing the impact of incidents on their recipients due to the technical security being employed across the RealVNC IT architecture. To ensure services will be available, an in house technical team monitoring the software infrastructure 24/7 to make sure vulnerabilities are mitigated.

Table 1: Reporting obligation

NIS2 Customer Requirement	When to report	What to report	RealVNC Response
A notification (for the recipients of services that are potentially affected by a significant cyber threat	Without undue delay	Any measure or remedies that those recipients are able to take in response to that threat; also inform those recipients of the significant cyber threat itself	RealVNC Connect allows for real time monitoring ensuring any reporting requirement timeframes are available – in this case 'without undue delay'.
An early warning (for CSIRT or competent authority)	Without undue delay and, in any event, within 24 hours of becoming aware of the significant incident	Indicates whether the significant incidents is suspected of being caused by unlawful or malicious acts or could have cross-border impact	RealVNC Connect can facilitate the collection and communication of early incident data ensuring the reporting obligations of 24 hours is followed.
An incident notification (for CSIRT or competent authority)	Without undue delay and, in any event, within 72 hours of becoming aware of the significant incident	Indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise	RealVNC Connect can facilitate the collection and communication of subsequent incident data aiding in the formation of impact severity within the 72 hour timeframe.
An intermediate report (for CSIRT or competent authority)	Upon the request of a CSIRT or the competent authority	Relevant status updates	The access to logs and other relevant data through RealVNC Connect can aid in the production of intermediate reports supporting the overall assessment and any relevant updates.
A final report (for CSIRT or competent authority)	Not later than one month after the submission of the incident notification	I. A detailed description of the incident, including its severity and impact; II. The type of threat or root cause that is likely to have triggered the incident III. Applied and ongoing mitigation measures	The overall ability for RealVNC to collect key data endpoints will help with the submission of an accurate final report alongside the information gathered from the reports produced in the early stages of the incident.

		IV. Where applicable, the cross-border impact of the incident	
A progress report (for CSIRT or competent authority)	In the event of an ongoing incident	Incident update	RealVNC Connect being a centralized remote access tool will aid in the updating of information through accurate data collection.