Cyber Security Document

SYNERGY IN ASSURANCE, STRENGTH IN COMPLIANCE®

Driving Compliance® in the new digital economy.

XGRC® SOFTWARE

Table of
Contents

Executive

Summary

At Strategix Application Solutions, safeguarding your data is our top priority. As the Original Equipment Manufacturer (OEM) of the XGRC® platform, we understand the critical role that data security plays in your organisation's success. Our commitment is to meet regulatory standards and actively anticipate and mitigate evolving threats, ensuring your data is protected at every level. The XGRC® platform is more than a software solution—it is a secure, resilient, and proactive tool designed to safeguard your business operations in today's complex digital landscape.

Our XGRC® platform is built to provide robust, secure, and compliant solutions that adhere to the highest industry standards. This dedication to excellence is validated by our ISO 27001:2022 certification, which serves as a benchmark for information security management. This certification underscores our ongoing commitment to maintaining the highest levels of security in every aspect of our platform—from design and development to support and delivery.

With comprehensive data protection controls embedded throughout the XGRC® platform, we ensure every client can confidently operate. Whether through secure data storage, advanced encryption protocols, or continuous compliance monitoring, our approach is designed to protect your data and empower your business to thrive. Strategix is committed to Driving Compliance® by offering a platform that is as secure as it is dynamic, giving you the peace of mind you need to focus on what truly matters—your business.

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi UKAS MANAGEMENT SYSTEMS

Click to view **Client Directory certificate**

Back

ISO 27001:
2022 Certification

We are proud to be ISO 27001:2022 certified, which underscores our dedication to maintaining a world-class Information Security Management System (ISMS). This certification covers the provisioning of design, development, delivery, and support for the XGRC® cloud-based platform, ensuring that our practices are aligned with the most stringent security standards globally.

Our certification ensures:
- Implementation of comprehensive security controls.
- Regular audits and continuous improvement of our ISMS.
- Full compliance with international standards, giving you peace of mind that your data is always secure.

This certification reflects an ongoing commitment to security excellence. Maintaining ISO 27001:2022 certification involves regular evaluations of our security practices, ensuring they evolve to address new threats and regulatory changes. By embedding these controls into every aspect of our operations—from design and development to support—we provide a resilient, reliable, and robust platform. This approach ensures that security needs are not only met today but that future challenges are also anticipated.

Data Security and
Privacy Controls

At Strategix, we recognise that your data is the backbone of your business, and we take every measure to ensure its safety. The XGRC® platform fully complies with the General Data Protection Regulation (GDPR) and the Protection of Personal Information Act (POPIA), adhering to the strictest global data privacy and protection standards. This ensures that all sensitive information is handled with care, securing your data at every stage of its lifecycle.

Your data belongs to you. When our business relationship ends, we return all data, ensuring its safe removal from our systems. As a testament to our commitment to security, we provide a Data Destruction Certificate, guaranteeing that all traces of your data have been securely destroyed. Furthermore, we leverage Microsoft Azure's Europe-West region to store data, utilising its advanced infrastructure to maintain high availability and security.

We employ 256-bit Rijndael encryption for all data, ensuring maximum security for data in transit, at rest, and within databases. With encryption keys unique to each customer, your data is protected against unauthorised access, ensuring confidentiality and security throughout its lifecycle. Our encryption protocols help reinforce trust in your data's integrity and protection.

Back

Network Security and
System Monitoring

Our network security framework is designed to prevent unauthorised access and continuously monitor potential threats. The XGRC® platform's architecture includes segregated system layers and restricted access to critical functions. We have implemented industry-leading security measures, such as server hardening and real-time monitoring, to maintain the integrity of our systems.

We employ advanced **Security Information and Event Management (SIEM)** tools to aggregate and analyze security events across our environments in real-time. In addition, our **Security Orchestration, Automation, and Response (SOAR)** capabilities enable us to automate security operations, ensuring rapid detection and response to incidents. Our **Security Operations Centers (SOC)** provide 24/7 monitoring, using real-time intelligence to identify and address potential threats proactively.

Our approach is built on the **NIST Cybersecurity Framework**, which provides a comprehensive structure for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. Additionally, our practices align with **OWASP Top 10** standards to address the most critical web application security risks. By incorporating the **CIS Controls** framework, we ensure that our defense mechanisms evolve to counter emerging threats, while the XGRC® platform remains monitored 24/7 to ensure proactive SOC, SIEM & SOAR incident response.

We conduct daily automated vulnerability assessments driven by AI models that constantly learn and adapt to emerging threats. These vulnerabilities are recorded in the XGRC® platform, where risk assessments are performed, action plans are initiated, and controls are implemented to mitigate risks. This process ensures the platform remains resilient against new and evolving cyber threats.

Response times for various security incidents and service issues are stipulated within our SaaS agreement, ensuring that all incidents are managed in accordance with predefined service levels. Our Incident Response Team follows documented and maintained procedures within the ISMS, providing every potential threat is met with a swift and decisive response.

Back

Enterprise

Architecture

The XGRC® platform is built on a scalable and secure architecture, leveraging Microsoft Azure's cloud infrastructure to ensure high availability, resilience, and security. The architecture is designed with key Azure services and other leading industry software that enable enterprise-grade performance and protection. Some of the core components include:

Cloudflare DNS and Web Application Firewall (WAF):
These services help manage secure routing and protect against common web vulnerabilities.

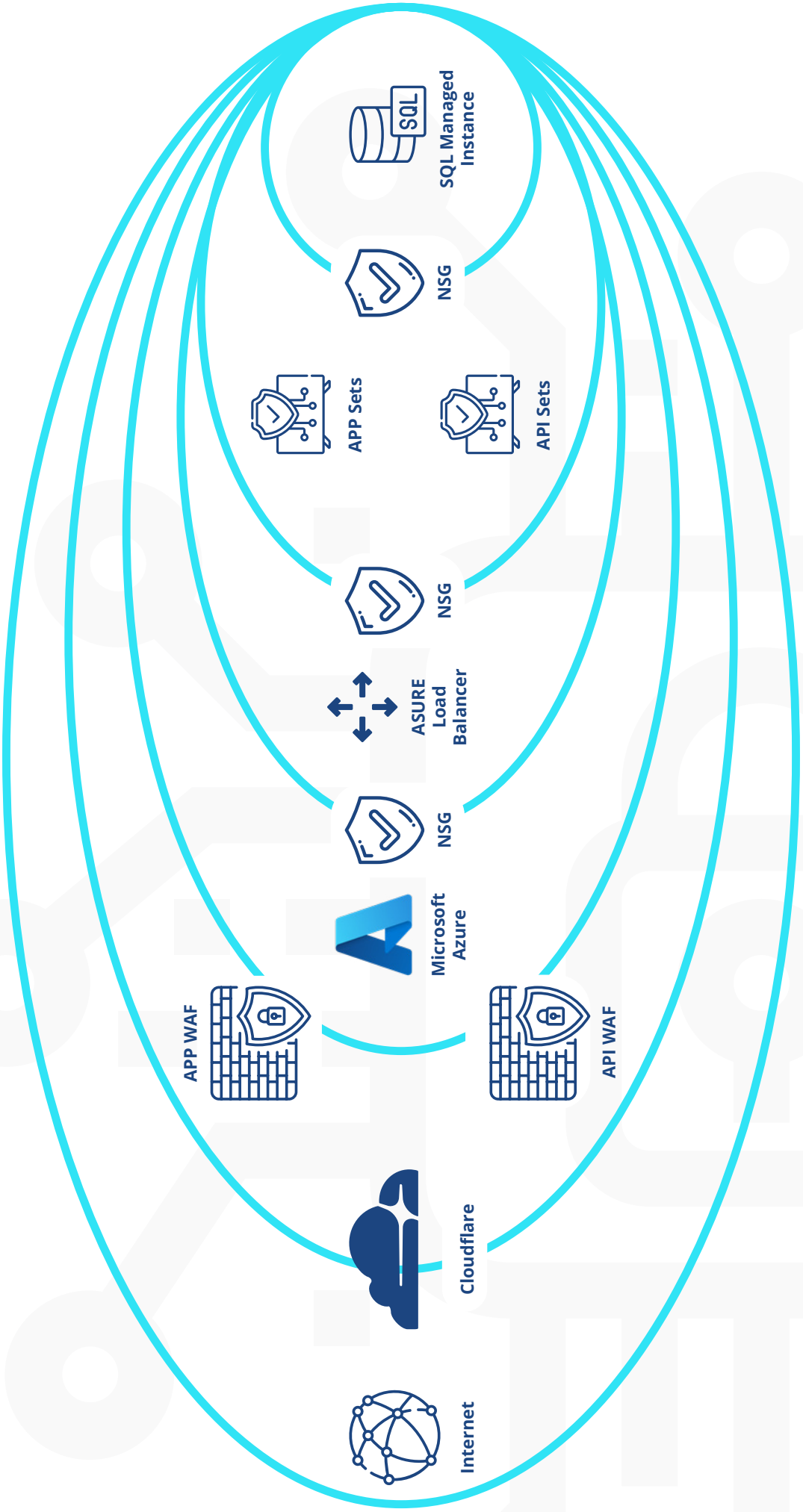
Azure Active Directory:
Manages identity and access controls, providing secure authentication for all users

Azure Load Balancer:
Ensures high availability by distributing network traffic across multiple servers.

Azure Managed SQL Instance:
Provides reliable and scalable data storage with advanced security features.

HakWare Archangel:
Advanced monitoring and assessment, ensuring continuous evaluation of potential vulnerabilities and security risks without compromising on efficiency.

This architecture allows XGRC® to offer robust, secure, and compliant solutions, integrating seamlessly with the financial industry's regulatory requirements. While we provide this high-level view of our architecture, detailed infrastructure maps are not shared to maintain the security integrity of our platform.


SQL Managed Instance
NSG
APP Sets
API Sets
NSG
ASURE Load Balancer
NSG
Microsoft Azure
APP WAF
API WAF
Cloudflare
Internet

Back

Incident Response and
Disaster Recovery

Our Incident Response Team operates under documented procedures within our ISMS, ensuring that every potential threat is met with a swift and decisive response. Incident classification and response times are clearly defined, with our team available to respond through various channels depending on the severity of the situation.

We conduct daily automated vulnerability assessments, driven by AI models that constantly learn and adapt to emerging threats. These vulnerabilities are recorded in the XGRC® platform, where risk assessments are performed, action plans initiated, and controls put in place. This proactive approach ensures that our platform remains resilient against new and evolving cyber threats.
High-Level Response Plan

Our incident response follows a structured, well-defined process, ensuring that potential security incidents are addressed quickly and effectively. The plan includes the following key phases:

1. **Identification:** Detect and determine the scope and severity of the incident.
2. **Containment:** Implement measures to limit the impact and prevent further damage.
3. **Eradication:** Eliminate the root cause of the incident.
4. **Recovery:** Restore affected systems and services to full functionality while ensuring that all vulnerabilities are mitigated.
5. **Lessons Learned:** Review the incident to identify improvements and strengthen future response efforts.

This plan ensures that incidents are handled swiftly, and our SaaS and EULA agreements provide further details on service levels and the responsibilities of both parties.

In terms of disaster recovery, we have implemented a comprehensive plan that includes daily backups, data replication across multiple locations, and regular testing. Our Recovery Point Objective (RPO) is 1 hour, ensuring minimal data loss, while our Recovery Time Objective (RTO) is 4 hours, allowing for swift restoration of services. Additionally, hourly log files ensure complete data integrity during restoration.

XGRC is designed to scale dynamically to handle high-demand periods or potential incidents. This ensures that even during times of unexpected traffic surges or stress on the system, additional resources are automatically allocated, maintaining our RPO and RTO targets. All disaster recovery procedures are tested quarterly, and the results are audited annually by an external ISO auditor, guaranteeing that systems are restored efficiently in any scenario.

Vendor Management
and Confidentiality

At Strategix, our vendors are critical in maintaining our security posture. Vendors engaged by Strategix are vetted in accordance with our ISMS processes, which are aligned with our ISO 27001:2022 certification. This ensures that all third-party vendors comply with GDPR, POPIA, and other relevant regulations. These vendors are audited annually as part of our continuous improvement process, ensuring that our entire supply chain upholds the same rigorous standards.

Confidentiality is at the core of our operations. Our SaaS agreement emphasises the importance of privacy and the protection of customer data. We have stringent measures in place to ensure that all personal information is handled with the utmost care, and we enforce strict non-disclosure agreements with all involved parties. Every step of the data journey is safeguarded, from collection to destruction, ensuring that your data is treated with the highest level of confidentiality and respect.

Maintaining a secure vendor network is an essential component of our strategy. Regularly assessing and collaborating with our vendors ensures that their security standards match our own. This cooperative approach strengthens the entire supply chain, reducing potential vulnerabilities and reinforcing our commitment to safeguarding client data.

Back

Support and
Maintenance

Our support services are designed to be both proactive and responsive, ensuring that issues are addressed efficiently before they escalate into more significant concerns. We offer multiple channels for clients to log support requests, and our dedicated team is committed to resolving issues within predefined timeframes.

Critical security patches are deployed immediately, outside of regular update cycles, to mitigate risks as they arise. By offering security updates with minimal or no operational disruption, we ensure the platform remains protected without impacting business continuity. This proactive approach keeps our clients one step ahead of potential security risks, ensuring that their data and operations remain secure at all times. Our SaaS and EULA agreements further detail the specific service levels and response protocols, ensuring transparency around our commitments to security and support.

Compliance
Monitoring

Compliance is embedded in every aspect of the XGRC® platform at Strategix. Our compliance monitoring system is regularly updated to align with changing regulations and industry standards. The platform's continuous compliance monitoring ensures that clients remain ahead of potential regulatory issues. At the same time, our alignment with international standards such as GDPR and POPIA helps to reduce the risks of fines or penalties.

We are committed to meeting current regulatory requirements and anticipating future compliance needs. Through continuous monitoring and regular updates, the XGRC® platform helps organisations stay compliant, reducing the burden on internal teams and allowing them to focus on their core business activities.

User Access
Management

User access management is one of the foundational pillars of security within the XGRC® platform. Administrators are empowered with granular controls to define user permissions down to the module, dashboard, and record level. These permissions include options for adding, editing, viewing, and deleting rights. Additionally, record-level security is maintained by configuring access to business units and categories, ensuring only authorised users can view or manipulate sensitive data.

At the customer level, access is controlled through the least access principle, meaning newly deployed features and modules default to no-access. This ensures that the system administrator only grants the necessary permissions, reducing the risk of unauthorised access. This principle ensures secure user management, even as the platform evolves to meet the changing needs of our clients.

Back

Appendix:

Overview of ISMS Documentation and Policies

To provide insight into the comprehensive nature of our Information Security Management System (ISMS), below is an overview of the key documents, policies, and checklists we maintain. These are not static documents but integral to the XGRC platform's functionality, ensuring that all governance, risk, and compliance (GRC) operations are executed and audited through the system.

- Information Security Policy
- ISMS Scope Document
- Corrective Actions Log
- Risk Assessment and Risk Treatment Process Document
- Statement of Applicability (SoA)
- Information Security Objectives
- Roles, Responsibilities, and Authorities Document
- Communication Plan
- Competence, Training, and Awareness Policy
- Documented Information Management Policy
- Operational Planning and Control Document
- Internal Audit Program
- Nonconformity and Corrective Action Process
- Continual Improvement Process
- Incident Management Policy
- Access Control Policy
- Supplier Security Policy
- Asset Management Policy
- Cryptography Policy
- Physical and Environmental Security Policy
- Communications Security Policy
- System Acquisition, Development, and Maintenance Policy
- Audit Checklist
- Information Security Incident Management Policy
- Business Continuity Management Policy
- Compliance Obligations and Legal Requirements Document
- Management Review Meeting Minutes
- Risk Treatment Plan
- Monitoring and Measurement Plan

These documents are maintained and implemented within the XGRC® platform, ensuring that all procedures, governance, risk management, and compliance tasks are carried out and continually audited. While these documents are essential to the ISMS process, we do not share them externally as they contain sensitive information that could compromise our security protocols.

Back

Conclusion

At Strategix Application Solutions, we believe that excellence in security and compliance is not a destination but a continuous journey. Our ISO 27001:2022 certified XGRC® platform is designed to provide your organisation with the assurance that your data is secure, compliant, and managed with the highest levels of integrity.

Through a combination of rigorous security controls, proactive incident response, and continuous compliance monitoring, we ensure that your organisation remains protected against evolving cybersecurity threats. Our platform is designed to support your business as it grows, adapting to changing regulatory landscapes and security challenges.

By partnering with Strategix, you are not only securing your data but also empowering your organisation to operate with confidence. With our Driving Compliance® philosophy, we deliver a platform that blends innovation with security, ensuring your organisation's operational resilience.

SYNERGY IN ASSURANCE, STRENGTH IN COMPLIANCE—Strategix Application Solutions proudly offers a trusted, comprehensive solution for all your governance, risk, and compliance needs.

Contact

Information:

+27 87 802 0179

XGRC SOFTWARE