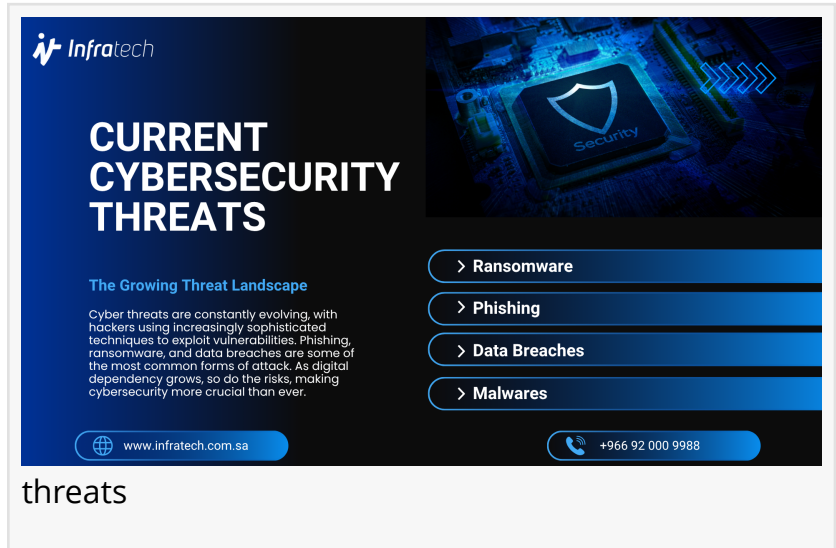


Infratech Helps Saudi Private Sector Prepare for NCNICC-1:2025 Cybersecurity Compliance

Infratech supports Saudi businesses with gap assessments, remediation, governance and evidence-based NCNICC-1:2025 compliance readiness.

RIYADH, SAUDI ARABIA, September 20, 2026 /EINPresswire.com/ -- [Infratech](https://www.infratech.com.sa), a Saudi cybersecurity and technology services provider, is helping private-sector organizations across the Kingdom prepare for the [National Cybersecurity Authority's NCNICC-1:2025](#) cybersecurity controls through structured assessments, remediation support and continuous compliance readiness.



threats

The Non-CNI Private Sector Entities Cybersecurity Controls, known as NCNICC-1:2025, establish minimum cybersecurity requirements for applicable private-sector organizations that are not classified as Critical National Infrastructure.

“

Compliance should not become a documentation exercise. NCNICC-1:2025 should translate into stronger security, clear ownership and measurable protection.”

Eng. Ayman Alsuhaime, CEO of Infratech

For Saudi businesses, understanding the framework is only the first step. The larger challenge is determining applicability, identifying gaps, implementing technical and governance controls, and maintaining evidence that demonstrates those controls are operating effectively.

“Infratech’s role is to help organizations move from understanding the regulation to actually implementing it,”

said Eng. Ayman Alsuhaime, CEO of Infratech. “Compliance should not become a documentation exercise. The controls should translate into stronger security, clearer ownership and measurable protection across the organization.”

From Requirement to Practical Implementation

NCNICC-1:2025 addresses cybersecurity across areas including governance, cyber defense, third-party relationships and cloud environments.

Organizations may need to examine policies and responsibilities, cybersecurity risk management, identity and access control, endpoint protection, vulnerability management, security monitoring, incident response, backups, supplier relationships and cloud security.

Infratech helps organizations translate these requirements into practical cybersecurity activities rather than treating the framework as a checklist.

The process begins by determining applicability and defining the scope of the environment.

This can include identifying relevant business units, systems and assets, reviewing cloud services and suppliers, documenting dependencies and understanding how cybersecurity responsibilities are currently managed.

Correct scoping helps organizations focus their resources on the systems, risks and controls that matter.

Gap Assessment and Remediation

Once the scope has been established, Infratech conducts structured gap assessments to compare an organization's current cybersecurity posture against NCNICC-1:2025 requirements.

Existing controls are reviewed to determine whether they are fully implemented, partially implemented or require remediation.

The findings can then be converted into a prioritized roadmap based on cybersecurity risk,



**INFRA TECH
IN THE
FOREFRONT**

Infratech has achieved the first level in the contractors classification of the cyber security

1
2
3 *First-Class Cybersecurity Ranking*
4
5

<https://infratech.com.sa>

Infratech Co Earns First-Class Cybersecurity Classification in Saudi Arabia

 **Infratech**

infratech

regulatory requirements, operational impact and implementation complexity.

Remediation may include developing or updating policies, defining cybersecurity roles and responsibilities, strengthening identity and access controls, improving vulnerability management, enhancing monitoring, developing incident-response procedures or implementing technical security measures.

The objective is to create a practical path toward compliance while simultaneously improving the organization's overall cyber resilience.

Evidence Is a Critical Part of Readiness

Cybersecurity compliance is not demonstrated by policies alone.

Organizations must also be able to show that required controls have been implemented and are operating in practice.

Evidence may include approved procedures, system configurations, access records, vulnerability reports, security logs, backup results, risk assessments, employee awareness records and management approvals.

Infratech helps organizations establish evidence structures that connect each applicable requirement with the implemented control and the records demonstrating its operation.

This can improve internal governance while making future compliance reviews and audit preparation more structured and efficient.

Connecting Compliance With Security Operations

Infratech's approach connects regulatory readiness with day-to-day cybersecurity operations.

The company provides services across Governance, Risk and Compliance, Managed Security Operations Center services, offensive security, incident response and digital forensics, security technologies and OT security.

This allows a compliance gap to be addressed through the appropriate cybersecurity capability rather than through documentation alone.

For example, requirements related to security monitoring may be supported through SIEM and managed security operations. Vulnerability-related requirements can involve assessments, penetration testing and remediation. Governance requirements may require defined ownership, policies, risk processes and management reporting.

By connecting governance with operational security, organizations can use NCNICC-1:2025 as an opportunity to strengthen cybersecurity across the business.

Third-Party and Cloud Cybersecurity

Modern organizations increasingly depend on cloud platforms, outsourced services, software providers and technology partners.

These relationships extend cybersecurity risk beyond the organization's internal infrastructure.

NCNICC-1:2025 includes cybersecurity requirements related to third parties and cloud services, making supplier and external-service governance an important part of compliance readiness.

Infratech helps organizations identify these dependencies, assess relevant risks and incorporate external providers into the wider cybersecurity governance framework.

Compliance Is Not a One-Time Project

Cybersecurity environments continuously change.

New employees join, systems are deployed, cloud services expand, suppliers change and new vulnerabilities appear.

For this reason, Infratech encourages organizations to treat NCNICC-1:2025 compliance as an ongoing cybersecurity program rather than a one-time certification exercise.

Periodic assessments, remediation tracking, control reviews, evidence maintenance and continuous monitoring can help organizations maintain readiness as their technology and risk environments evolve.

“Organizations should use NCNICC-1:2025 as an opportunity to strengthen how cybersecurity operates across the business,” Alsuhaimeh added. “When governance, technical controls and evidence work together, compliance becomes an outcome of good cybersecurity rather than a separate exercise.”

Supporting Saudi Cybersecurity Readiness

NCNICC-1:2025 reflects Saudi Arabia's continued development of a structured national cybersecurity environment and creates an opportunity for private-sector organizations to strengthen governance and improve resilience.

Infratech supports organizations from initial applicability assessment and gap analysis through remediation planning, control implementation, evidence preparation and ongoing compliance

readiness.

Organizations can contact Infratech to evaluate their current cybersecurity posture and develop a practical NCNICC-1:2025 compliance roadmap.

About Infratech

Infratech is a Saudi cybersecurity and technology services company headquartered in Riyadh.

The company provides services across Governance, Risk and Compliance, managed security operations, offensive security, incident response and digital forensics, cybersecurity technologies, OT security, cybersecurity awareness and advisory services.

Infratech supports government and private-sector organizations in strengthening cybersecurity resilience, meeting regulatory requirements and protecting critical business operations.

For more information, visit [www.infratech.com.sa](<http://www.infratech.com.sa>).

Ayman Al Suhaim

Infratech

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/943725307>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.