

04 • CERTIFY

Threat, vulnerability and risk assessment for data centres

A facility can hold a TIA 942C Facility Certificate and still have significant operational vulnerabilities. A TVRA confirms it is being operated safely, securely, and resiliently.

WHAT THIS SERVICE COVERS

Infrastructure certification confirms the physical systems were built to standard. A TVRA confirms the facility is being operated safely, securely, and resiliently.

The Threat, Vulnerability and Risk Assessment covers all twelve operational assessment domains: organisational security, physical security, electronic security, emergency preparedness, fire protection, energy supply, HVAC and cooling, construction integrity, water infiltration risk, transport and access, location risk, and telecom infrastructure. The assessment combines a desktop review of documentation and procedures with an on-site physical inspection and structured staff interviews. Each finding is rated by severity with a specific corrective action recommendation, and a stakeholder workshop follows to present findings and agree priorities. An optional failover testing component goes beyond documentation review to physically test whether critical infrastructure failover happens as specified.

All 12 assessment domains

On-site physical inspection included

Prioritised CAPA, quantified ratings

WHAT WE DELIVER

Deliverables from this engagement

01

Assessment Reports, All 12 Domains

Structured assessment report per domain, covering documentation review findings, on-site inspection findings, and gap analysis against best practice.

02

On-Site Inspection Report

Physical inspection covering infrastructure condition, security perimeter, signage, access control, fire suppression readiness, and maintenance deficiencies.

03

Documentation Review Summary

Assessment of operational procedures, emergency response plans, maintenance records, training records, and incident logs against each domain's requirements.

04

Stakeholder Workshop

Facilitated workshop presenting findings and agreeing the corrective action plan, attended by operations, security, and management representatives.

05

Prioritised Corrective Action Plan

Structured CAPA with each finding classified by severity, a specific recommendation, estimated effort, and suggested resolution timeline.

06

Optional Failover Test Reports

Physical testing of critical infrastructure failover, generator changeover, UPS transfer, cooling backup, confirming timeframes are met.

WHY TECHNAVIOUS

What makes our TVRA more useful than a checklist review

1 On-site physical inspection as standard

Documentation review alone does not capture what is actually happening in the facility. On-site inspection identifies maintenance deficiencies, access control gaps, and physical security vulnerabilities not reflected in any document.

2 Failover testing as a value-add option

Most TVRA assessments review procedures but do not physically test failover. Our optional component physically initiates generator changeover, UPS transfer, and cooling backup, confirming actual performance against specified times.

3 Quantified risk ratings, not qualitative judgements

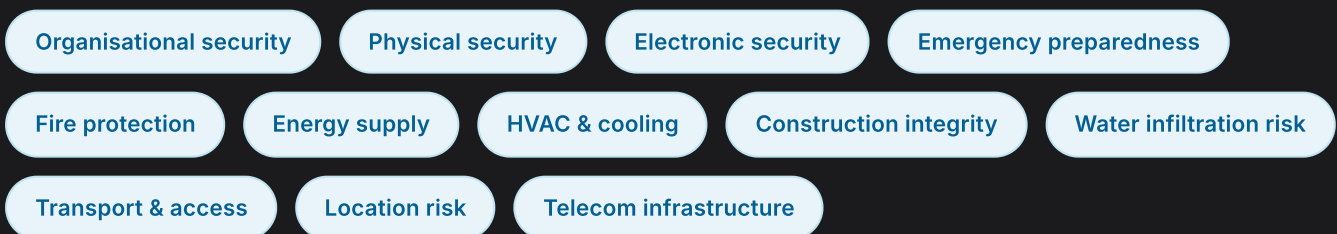
Every finding is assigned a quantified risk rating based on probability and potential impact, letting the client prioritise corrective actions by actual risk exposure.

HOW WE WORK

Four phases from scoping to CAPA delivery

01	02	03	04
Scoping	Assessment	Analysis	Workshop & CAPA
Assessment scope and domains confirmed. Documentation list requested. Site visit scheduled.	Desktop documentation review and on-site physical inspection conducted across all 12 domains.	Findings analysed, risk-rated, and cross-referenced. Corrective action recommendations developed.	Stakeholder workshop conducted. Prioritised CAPA delivered and agreed with client.

THE 12 ASSESSMENT DOMAINS



CASE STUDIES

Assessment and compliance work we have delivered

PRIVATE SECTOR BANK

DC health-check and operations assessment across 40+ infrastructure tests and an eight-category O&M process audit. 500+ days of uninterrupted operations and 100% SLA performance achieved following remediation.

AUTOMOBILE MANUFACTURING PLANT

DC audit after planned UPS maintenance took 40–50% of racks offline for 8–9 hours. Root cause corrected across all 50 racks, with full N+1 redundancy restored.

INFRASTRUCTURE PROJECT CLIENT

Risk assessment of pending post-IST documentation, commissioning reports, and handover packages. All four high-risk documentation streams reduced to low risk with measurable closure milestones.

FREQUENTLY ASKED QUESTIONS

Questions we are regularly asked about TVRA

What is the difference between a TVRA and a TIA 942C audit?

TIA 942C validates that infrastructure was built to standard and meets its rated level. A TVRA assesses how the facility is operated: security posture, emergency preparedness, and maintenance practices. A facility can hold a TIA 942C certificate and still have vulnerabilities only a TVRA would identify.

How often should a TVRA be conducted?

Most organisations conduct an annual or biennial TVRA as part of their risk management programme. The appropriate frequency depends on the pace of change and any tenant or regulatory requirements. We recommend an initial full assessment followed by a lighter annual review.

Can we commission a TVRA without also purchasing TIA certification?

Yes. TVRA is an independent service commonly used as a standalone risk management tool, a pre-certification preparation step, or a tenant due diligence response.

What is the optional failover testing component?

It physically initiates generator changeover, UPS transfer, and cooling backup scenarios, recording actual response times against specified parameters, with the facility's operations team present.

Ready to scope your TVRA?

Tell us your facility size, the scope of assessment required, and whether you need failover testing included.

[Talk to us today](#)