



Cognizant Integrated Risk Management

Overview

Public sector organizations must safeguard sensitive data, ensure service continuity, and meet stringent oversight requirements—often with distributed teams, legacy systems, and constrained budgets. Cognizant's Integrated Information Risk Management provides a unified, proactive approach to identify, assess, mitigate, monitor, and report risks across enterprise, operational, cyber, compliance, and third party domains—enabling trust, transparency, and resilient service delivery.

Challenges (Public Sector)

- **Fragmented Governance:** Siloed risk processes across departments, programs, and vendors.
- **Evolving Mandates:** Continuous alignment to frameworks (e.g., NIST, ISO, GDPR, DPDP (India), sector standards like HIPAA, CJIS).
- **Limited Real Time Visibility:** Inadequate telemetry on control effectiveness and emerging risks.
- **Legacy & Hybrid Estates:** Complex mix of on prem, cloud, and citizen facing systems.
- **Resource Constraints:** Manual workflows, limited skills capacity, and high audit overheads.
- **Third Party Exposure:** Expanding reliance on partner ecosystems and mission critical vendors.

Solution (Public Sector)

Risk management is not just a compliance function—it's a strategic enabler for resilience and trust. At Cognizant, we embed risk intelligence across the enterprise to anticipate threats, align with global regulations, and empower confident decision-making. Our approach emphasizes proactive detection over reactive response, integrated governance across cyber, operational, and third-party domains, and regulatory alignment by design. We operationalize risk through meaningful KPIs and dashboards, build resilience into core processes, and leverage AI and automation to enhance—not replace—human judgment. This philosophy transforms risk from a siloed activity into a unified, value-driven capability.



Proactive over Reactive

Risk is best managed before it materializes. We prioritize early detection, predictive modeling, and continuous monitoring

Regulatory Alignment by Design

Compliance is embedded into our risk architecture, mapped to global standards (ISO, NIST, GDPR, RBI, SEBI) and tailored to client geographies

Resilience as a Mandate

Beyond risk avoidance, we build organizational resilience—ensuring continuity, adaptability, and stakeholder trust in the face of disruption



Integrated Governance

Risk is not siloed—it spans cyber, operational, third-party, and strategic domains. Our frameworks unify these dimensions for holistic oversight

Metrics that Matter

We operationalize risk through audit-ready KPIs, outcome-driven dashboards, and domain-specific taxonomies that speak to executives, auditors, and operations alike

Technology-Enabled Judgment

We leverage GenAI, automation, and analytics to enhance—not replace—human insight in risk decisions

Key Capabilities

- Risk Identification & Classification across programs, systems, and third party services.
- Quantitative & Qualitative Assessment using standardized scoring
- Controls Design & Implementation (preventive, detective, corrective) with accountability and SLAs.
- Continuous Monitoring with automated alerts, thresholds, and escalation paths.
- Dashboards & Reporting tailored for executives, program leads, and auditors.
- Compliance Management mapped to NIST, ISO, GDPR, DPDP (India), HIPAA, CJIS, and local regulations.
- Incident Learnings & Maturity Evolution integrated into governance for continuous improvement.
- Third Party Risk Management from onboarding to ongoing assurance and remediation.

Public Sector Use Cases

- Agency Wide Risk Register & Heatmap for a consolidated risk posture.
- Program Compliance & Audit Readiness with evidence backed control reports.
- Critical Service Continuity (public health, utilities, transportation, citizen portals).
- Third Party Due Diligence & Monitoring for vendors supporting mission critical functions.
- Cyber Risk Quantification to prioritize investments and brief leadership.
- Policy to Control Mapping for rapid regulatory alignment and demonstrable assurance.

Our Offerings:

Activate & Integrate

- Establish governance, roles, and RACI; deploy standardized frameworks and templates.
- Integrate with existing systems, SIEM/GRC platforms, and agency data sources.

Mitigate & Monitor

- Implement controls, define SLAs, and automate telemetry collection.
- Monitor KRIs/KPIs, trigger escalations, and track residual risk.

Optimize & Evolve

- Leverage AI/automation to reduce manual effort and improve consistency.
- Scale across departments and vendors; refine thresholds and playbooks.



Assess & Classify

- Build risk inventories across domains; apply consistent taxonomies and rating scales.
- Identify control gaps and prioritize treatment plans.

Report & Improve

- Deliver executive dashboards and audit ready evidence packages.
- Run post incident reviews, maturity assessments, and governance refresh cycles.

Benefits:

Functional



End to End Risk Management across enterprise, cyber, operational, compliance, and third party domains.



RealTime Visibility with predictive insights to pre-empt disruptions.



Unified Governance Framework that standardizes policies, processes, and artifacts.

Deployment



Accelerated Implementation using pre built templates, playbooks, and taxonomies.



Streamlined Workflows through automation and role based accountability.



Audit Ready Reporting with evidence traceability and version control.

Commercial / Mission Outcomes



Lower Compliance Overheads and reduced audit cycles.



Reduced Financial & Reputational Exposure through prioritized remediation.



Better Resource Utilization and faster time to assurance for citizen services.

Engagement Model & Pricing

Engagement Flow: Consultation → Needs Assessment → Proposal → Execution → Ongoing Assurance

Pricing Models: Fixed Price | Time & Material | Unit Based (e.g., controls attested, assessments completed)

Delivery Models: Dedicated (Onshore/Offshore/Nearshore) | Hybrid | Shared

Why Choose Cognizant

Cognizant brings deep expertise in Governance, Risk, and Compliance, backed by globally recognized certifications and proven success in transforming risk management for highly regulated environments. Our approach is technology-agnostic, integrating seamlessly with existing platforms while leveraging AI-driven accelerators for speed and consistency. With 24x7 global delivery through Centers of Excellence, we ensure measurable outcomes—reducing critical risks, achieving audit readiness, and aligning risk strategies with organizational objectives. Trusted by public sector agencies and Fortune 500 enterprises alike, Cognizant combines domain knowledge, innovation, and operational excellence to deliver resilient, compliant, and future-ready risk management solutions. To know more, please contact – cybersecuritypulse@cognizant.com

Cognizant helps engineer modern businesses by helping to modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. To see how Cognizant is improving everyday life, visit them at www.cognizant.com or across their socials [@cognizant](https://www.instagram.com/cognizant).

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB England
Tel: +44 (0)1 020 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraiyakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (0)1 44 4209 6060

APAC Headquarters

1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Tel: +65 6812 4000

© Copyright 2025–2027, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission of Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned here in are the property of their respective owners.

