Security & Resilience Overview

Building Trust & Resilience in the Travel Industry

Published March 2026

Internova TRAVEL GROUP

Contents

Executive Summary

At Internova Travel Group, security, privacy, and operational resilience are foundational to our mission. Our comprehensive security and risk management program is built on internationally recognized standards and a robust AI governance framework. We are committed to transparency, continuous improvement, and delivering reliable, secure travel management services so you can focus on your business with confidence. This document applies to the Internova brands listed below.

ALTOUR

yes your event solutions

GLOBAL TRAVEL COLLECTION

IN THE KNOW EXPERIENCES

The VACATION Group

TRAVEL LEADERS NETWORK

BarrheadTravel

nexion TRAVEL GROUP

Andrew Harper®

About Internova Security & Resilience

Internova Travel Group is a global leader in travel management, dedicated to protecting client data, ensuring operational continuity, and maintaining regulatory compliance across all brands and services. Our security and resilience strategy is built on a layered, integrated approach that leverages internationally recognized standards and frameworks, tailored for the unique needs of the travel industry.

- **ISO Standards:** Internationally recognized standards that form the foundation of our processes, controls, and continuous improvement cycles (e.g., ISO 27001 for information security, ISO 31000 for risk management, ISO 22301 for business continuity, ISO 42001 for AI management).
- **NIST Frameworks:** The NIST Cybersecurity Framework and NIST SP 800-53 provide detailed, control-based guidance for cybersecurity, privacy, and technology risk management.
- **COBIT 2019:** An IT governance and enterprise risk management (ERM) framework that includes security components. COBIT ensures that information and technology processes, risk, and value delivery are aligned with business objectives and regulatory requirements. It bridges enterprise risk (COSO/ISO) and technical controls (NIST/ISO), providing a holistic, end-to-end governance structure.
- **COSO ERM:** Supports strategic alignment and board-level oversight by integrating risk management with governance, culture, and performance.
- **OWASP:** The Open Web Application Security Project (OWASP) is a community-driven resource that provides best practice guidelines, technical standards, and maturity models for application, API, and AI security. While not a formal framework, OWASP's resources (such as the OWASP Top 10 and ASVS) are widely adopted and incorporated into our secure software development and AI risk management programs.

Our Approach Ensures

- **Comprehensive Coverage:** Security, privacy, and resilience controls are mapped to the specific risks and regulatory requirements of the travel management sector, including client data protection, third-party integrations, and decentralized advisor operations.
- **Operational Continuity:** Business continuity and disaster recovery are fully integrated, ensuring uninterrupted service and rapid recovery from disruptions.
- **Vendor & Supply Chain Resilience:** Regular risk assessments and business continuity requirements are enforced for all third-party partners and suppliers.
- **Continuous Improvement:** Ongoing monitoring, testing, and management reviews drive the evolution of our controls and processes, keeping pace with emerging threats and regulatory changes.

By aligning our security and resilience programs with these leading frameworks and tailoring them to the realities of travel management, Internova provides clients and partners with confidence in the integrity, reliability, and compliance of our services.

Our Commitment to Customers & Partners

- **Trust:** We prioritize the confidentiality, integrity, and availability of your data.
- **Transparency:** We provide clear reporting and documentation on our security and AI governance practices.
- **Compliance:** Our policies and controls are designed to meet or exceed regulatory requirements (e.g., GDPR, CCPA).
- **Continuous Improvement:** We regularly review and enhance our controls to address evolving risks.

Enterprise Resilience: Strategy and Structure

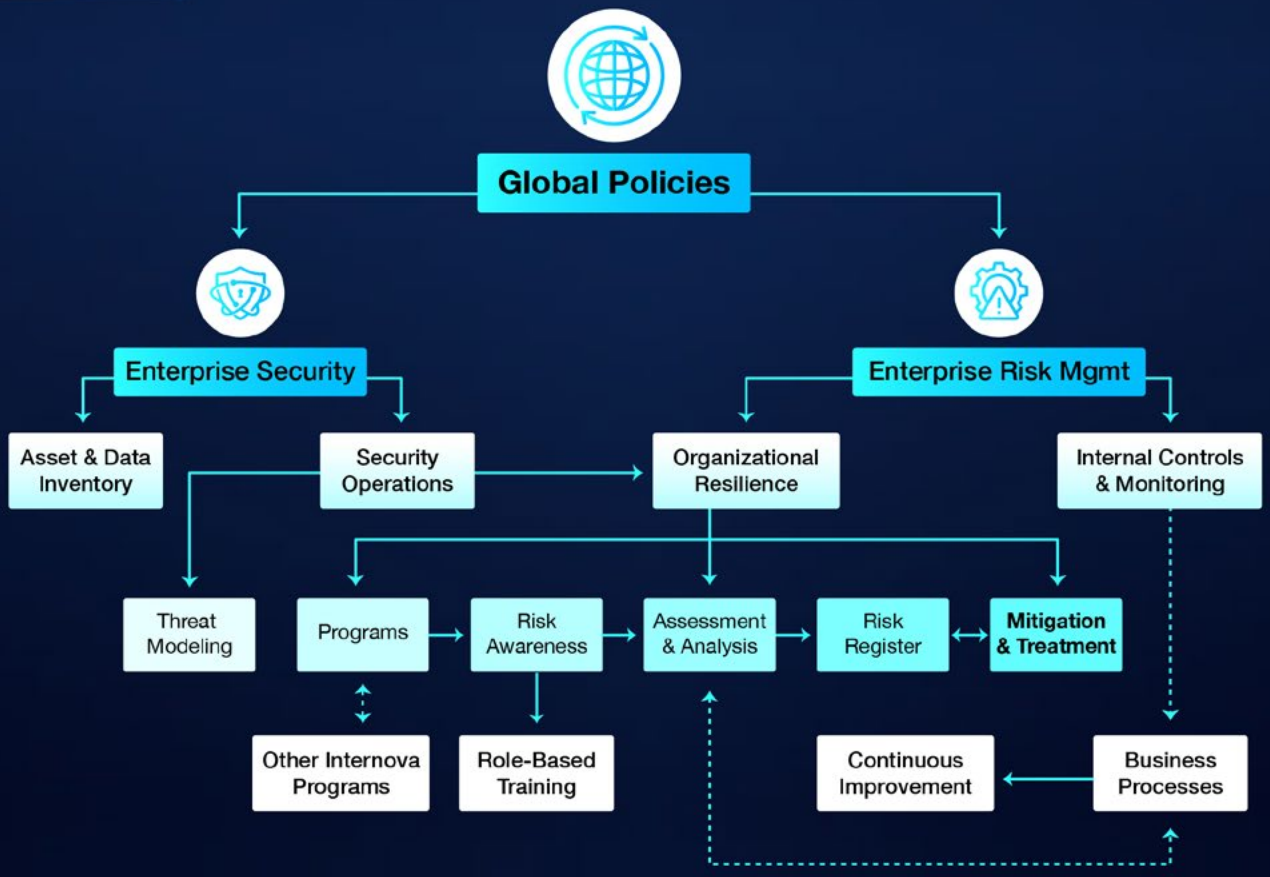
Enterprise resilience at Internova means anticipating, preparing for, and adapting to both incremental changes and sudden disruptions. Our approach ensures the continuity of critical travel management services and the protection of client data.

Key Areas of Resilience

- **Information Security:** Protecting data and systems in line with ISO 27001, NIST CSF, and COBIT.
- **Organizational Resilience:** Adapting to disruptions such as cyberattacks, pandemics, or supply chain issues.

Workflow Diagram

The diagram below illustrates how Internova integrates enterprise security and risk management under global policies, connecting asset and data inventory, security operations, and internal controls with organizational resilience activities. The workflow emphasizes a cycle of risk awareness, assessment and analysis, risk register maintenance, mitigation and treatment, and continuous improvement, ensuring that business processes remain robust and adaptive to evolving threats.



- **Business Continuity:** We are finalizing robust crisis management and recovery plans to ensure the continuity and rapid restoration of critical services. These plans will be subject to regular testing and continuous improvement.
- **Disaster Recovery:** Our IT systems are being enhanced for rapid recovery and secure remote access and will undergo annual testing upon completion.
- **Vendor & Supply Chain Resilience:** Regular risk assessments with business continuity and disaster recovery requirements for third-party partners.

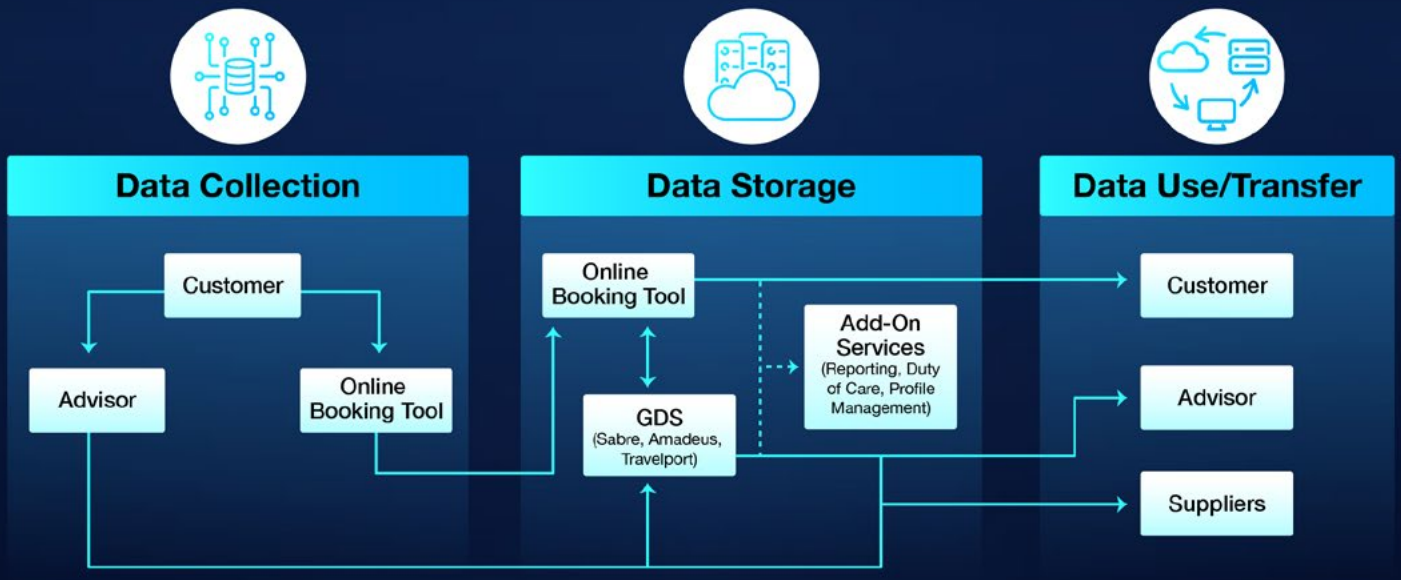
Information Security & AI Governance

Security Architecture & Dataflow Overview

Internova Travel Group's information security program is built on a layered, defense-in-depth architecture aligned with ISO 27001/27002, NIST CSF, and COBIT standards. To provide transparency into how we protect customer and partner data, the diagram below illustrates the flow of data through our systems, from initial collection to secure storage, processing, and eventual disposal.

Dataflow Diagram

The diagram below illustrates how customer and partner data flows through Internova's travel management systems, highlighting key security controls at each stage, including data classification, encryption, access controls, monitoring, and secure interfaces with third-party partners. This visual representation demonstrates our commitment to safeguarding sensitive information throughout its lifecycle.



Information capture/stored: Name, job title, company email address, mailing address, delivery address, phone numbers, airline, hotel, or car preferences, frequent flier/reward cards, hotel airport, seating preferences, meal preferences, billing info, credit card numbers (stored in accordance with PCI DSS requirements; only partial PAN is retained where required for business operations), passport/visa information, gender, date of birth.

Comprehensive Security Program

Aligned with ISO 27001/27002, NIST CSF, and COBIT, covering access control, incident management, vulnerability management, and continuous monitoring as well as endpoint and network protection programs.

- **Access Control:** Role-based access, least privilege, and multi-factor authentication is enforced.
- **Vulnerability Management:** Continuous vulnerability scanning and patch management are conducted to proactively address risks.
- **Endpoint, Device & Ransomware Resilience Program:** Utilizing XDR, Endpoint encryption and Zero Trust to protect endpoints and devices from malware and unauthorized access and provide recoverability in the event of ransomware or destructive incidents.
- **Network, Email & Perimeter Protection Program:** Reduce risk from common inbound attack vectors; phishing/email threats, drive-by downloads/web-based phishing, denial-of-service events, and general perimeter exposure through layered preventative and detective controls.
- **Continuous Monitoring:** 24/7/365 Security Operations Center. Security events and key risk indicators are monitored in real time, with automated alerting and regular reviews.
- **Penetration Testing:** Structured penetration tests are performed to validate the effectiveness of preventive and detective controls, identify exploitable paths (application, infrastructure, cloud, and user-driven attack vectors), and prioritize remediation based on business risk. Findings are tracked through to closure with validation/re-testing to confirm risk reduction.
- **Red & Purple Team Exercises:** Adversary-emulation (red team) and collaborative detection-and-response validation (purple team) exercises are conducted to assess real-world resilience across people, process, and technology. These exercises strengthen detection engineering, incident response workflows, and control effectiveness by validating end-to-end scenarios and driving measurable improvements.
- **Tabletop Exercises:** Scenario-based tabletop exercises are used to rehearse decision-making, escalation paths, communications, and cross-functional coordination for high-impact cyber events (including AI-related scenarios where applicable). Outcomes are captured as after-action improvements, playbooks, roles/responsibilities, and response procedures to continually improve readiness.

AI Governance

Our AI Governance Policy ensures responsible development, deployment, and management of AI systems, with commitments to transparency, risk and bias assessments, and compliance with emerging regulations.

- **Responsible AI:** Our AI Governance Policy ensures responsible development, deployment, and management of AI systems, with commitments to transparency, risk and bias assessments, and compliance with emerging regulations.
- **AI Model Security:** Regular testing for vulnerabilities, bias, and robustness against adversarial threats is performed on all AI models.

Incident Response

Rapid detection, escalation, and remediation of security events, including those involving AI.

Secure Software & API Development

- **Secure SDLC:** All software, including AI-powered applications, is developed using secure coding practices, vulnerability scanning, and automated testing, following ISO, NIST, COBIT, and standards and OWASP best practices.
- **Application & API Security:** All applications and APIs are developed and tested in accordance with the OWASP Top 10, ASVS, and Internova's Secure SDLC. Our API security program is aligned with the OWASP API Security Top 10, ensuring

robust protection for all integrations. Regular penetration testing and code reviews are conducted to identify and remediate vulnerabilities. Secure API development and monitoring are integral to our process.

- **AI Model Security:** Regular testing for vulnerabilities, bias, and robustness against adversarial threats.
- **Change Management:** All changes to applications and AI systems undergo risk assessments and cross-functional reviews.

Data Privacy, Protection & Classification

- **Comprehensive Data Protection:** Data privacy policies apply to all systems, including AI, and cover data classification, access controls, encryption, and compliance with regulations (GDPR, CCPA).
- **Data Classification:** Internova classifies data into four categories: Public, Internal, Confidential, and Restricted. Controls are tailored to the sensitivity of each category.
- **Privacy by Design:** Privacy requirements are embedded into the design and development of all systems and processes, ensuring compliance with GDPR, CCPA, and other regulations.
- **Vendor Management:** Third-party partners must meet our privacy and security standards, including AI-related services.
- **Data Retention & Disposal:** Data is retained and disposed of in accordance with regulatory and contractual requirements.

Risk Management & Continuous Improvement

- **Integrated Risk Management:** Risks from IT, operations, vendors, and AI are tracked in a central risk register, with controls mapped to ISO 31000, COSO, ISO 22301 standards and OWASP best practices.
- **Continuous Monitoring:** Key risk indicators and control effectiveness are regularly reviewed and reported.
- **Ongoing Improvement:** Regular exercises, audits, and management reviews ensure our controls remain effective and up to date.

Certifications, Audits & Compliance

Certifications obtained or pursued by Internova Travel Group, such as PCI DSS, ISO 27001, and EcoVadis, serve to independently validate our commitment to robust security, privacy, and sustainability practices. These certifications provide assurance to our customers and partners that our controls and processes meet rigorous international standards and industry best practices.

Current Certifications

- **PCI DSS 4.0.1:** Internova has achieved PCI DSS 4.0.1 Attestation of Compliance (AOC) at Level 1 and routinely undergoes independent third-party audits to verify the effectiveness of our security and privacy controls.
- **EcoVadis:** Internova's EcoVadis certification demonstrates our commitment to sustainability and corporate social responsibility by meeting internationally recognized standards for environmental, social, and ethical performance in our business operations.

Certifications in Progress

- **ISO 27001:** Internova is also pursuing ISO 27001 certification to further demonstrate our commitment to international best practices.
- **ISO 27701:** Internova is pursuing ISO 27701 certification to strengthen its privacy information management system, demonstrating a proactive approach to protecting personal data and supporting compliance with global privacy regulations.

Compliance

Our practices are designed to meet or exceed requirements under GDPR, CCPA, and other relevant regulations.

Audit Frequency

Independent assessors audit security and privacy controls at least annually. Annual audits include PCI DSS, and independent reviews of our security and privacy controls.

Security Controls Mapping

Control Domain	ISO 27001/ 27002/ 27701/ 42001/ 22301	NIST CSF / 800-53 / AI RMF	COSO ERM	OWASP
Access Control	5.15–5.17, 8.2, 27701-6.3	PR.AC, AC-2, AC-3, IA-2, IA-5	Control Activities	Top 10: A01, ASVS V4, SAMM
Data Encryption & Protection	8.24–8.28, 27701-6/8, 42001-6.3	PR.DS, SC-13, SC-28, AI RMF MG2	Information & Reporting	Top 10: A02, ASVS V9, SAMM
Incident Response	5.25, 5.26, 42001-8.2, 22301-8.4	RS.RP, IR-4, IR-5, AI RMF RM3	Review & Revision	Top 10: A09, SAMM, Testing Guide
Vendor Management	5.19, 5.20, 27701-7.2, 42001-7.2	ID.SC, SR-3, SR-5, AI RMF MG3	Risk Assessment	SAMM, Vendor Min Req
Application & API Security	8.28–8.34, 42001-6.4, 27034	PR.IP, SI-2, SA-11, AI RMF MG4	Control Activities	Top 10: A03–A10, ASVS, API Top 10
Business Continuity	5.29, 8.4, ISO 22301	CP-1, CP-2, CP-4, CP-9	Review & Revision	SAMM, Testing Guide
Risk Assessment & Management	6.1, 8.2, 42001-8.1, 31000, 27005	ID.RA, RA-3, RA-5, AI RMF RM1	Risk Assessment	SAMM, Risk Assessment Guide
Secure SDLC & Change Management	8.28, 8.32, 42001-6.5, 27034	PR.IP-3, CM-3, SA-10, AI RMF MG5	Control Activities	ASVS, SAMM, SDLC Policy
Vulnerability Management	8.8, 8.28, 42001-6.6	PR.IP-12, RA-5, SI-2, AI RMF MG6	Control Activities	Top 10: A06, Testing Guide
Endpoint/Network Security	8.10–8.13, 8.21, 8.22	PR.PT, SC-7, SC-18, SI-4	Control Activities	Top 10: A05, A06, SAMM
Continuous Monitoring & Logging	8.15, 8.16, 5.25–5.26, 42001-8.3	DE.CM, AU-2, AU-6, SI-4, AI RMF MG7	Info & Communication	Top 10: A09, ASVS V10, SAMM
Data Privacy & Classification	5.12, 5.13, 8.2, 27701-6/8, 42001-6.3	PR.DS, DM-1, PL-2, AI RMF MG8	Information & Reporting	Top 10: A02, SAMM, Privacy Guide
AI Governance	42001-5, 42001-6, 42001-7, 42001-8, 27001-6.1, 27701-6/8	AI RMF (all), NIST CSF GV, ID, PR, RM	Governance & Culture, Risk Assessment, Review & Revision	OWASP LLM Top 10, GenAI Compass
AI Risk & Bias Assessment	42001-8.1, 27701-8, 27001-6.1	AI RMF RM1, RM2, RM3	Risk Assessment	OWASP LLM Top 10, AI Risk Guide
AI Model Security	42001-6.4, 42001-8.2	AI RMF MG4, MG6	Control Activities	OWASP LLM Top 10, GenAI Compass
AI Change Management	42001-6.5, 42001-8.3	AI RMF MG5, MG7	Control Activities	OWASP LLM Top 10, SAMM
AI Documentation & Inventory	42001-7.1, 42001-7.2	AI RMF MG3, GV	Information & Reporting	OWASP LLM Top 10, GenAI Compass
AI Vendor/Third-Party Risk	42001-7.2, 27701-7.2	AI RMF MG3, SR-3	Risk Assessment	OWASP LLM Top 10, Vendor Min Req
Training & Awareness	7.2, 42001-6.7, 27001-7.2	PR.AT, AT-2, AI RMF GV	Governance & Culture	SAMM, Training Guide
Logging & Monitoring Failures	8.15, 8.16, 5.25–5.26	DE.CM, AU-2, AU-6, SI-4	Info & Communication	Top 10: A09, Testing Guide
Input Validation & Injection	8.28	PR.IP, SI-10	Performance	Top 10: A03, Cheat Sheets
Authentication & Session Management	5.16–5.17	IA-2–IA-5, PR.AC	Control Activities	Top 10: A07, Cheat Sheets
Secure Design	8.25, 8.28	PR.IP	Control Activities	Top 10: A04, ASVS
Security Misconfiguration	8.9, 8.28	PR.IP	Control Activities	Top 10: A05, ASVS
Software/Data Integrity	8.28	SI, PR.IP	Control Activities	Top 10: A08, ASVS
SSRF & API Security	8.28	PR.IP	Control Activities	Top 10: A10, API Top 10

Training and Awareness

All staff receive annual security and privacy training, with specialized modules for developers, administrators, and executives. Ongoing awareness campaigns and targeted training ensure that security and privacy are embedded in our culture.

Personnel Screenings

All staff undergo pre-employment screenings, which may include verification of employment history, references, education credentials, and criminal background checks. Screening procedures and methods may vary for employees inside and outside the United States, as required by applicable local laws.

What this Means for You

- **Peace of Mind:** Your data and travel operations are protected by industry-leading security and resilience practices.
- **Regulatory Confidence:** Our compliance with global standards helps you meet your own regulatory obligations.
- **Reliable Service:** Implementation of business continuity and incident response to ensure uninterrupted service, even during disruptions.
- **Transparent Partnership:** We provide clear, client-facing reporting and are always available to discuss our security posture.

Key Takeaways

- Internova's resilience covers all aspects of security, data privacy, and AI governance.
- Our AI Governance Policy ensures responsible, secure, and ethical use of AI.
- We are committed to transparency, compliance, and continuous improvement to protect our clients and partners.

For more information, to request detailed documentation (such as policy excerpts), visit our Trust Center at trust.internova.com.