Integrated Management System Policy

Risk & Compliance

Class 1 – General B2B Use / Public

Version 1.0 - 06/05/2026

Contents

Version Control

Current Version

Parameter	Value
Current Version	1.0
Release Date	06/05/2026
Author	Shannon Huxley, Head of Risk and Compliance

Version History

Version	Date	Author	Description of Changes
0.1	06/05/2026	Shannon Huxley, Head of Risk and Compliance	DRAFT
0.2	06/05/2026	Shannon Huxley, Head of Risk and Compliance	QA & SIGN OFF
1.0	06/05/2026	David Senior, Chief Finance Officer	PUBLISHED

1 Purpose & Objectives

The purpose of this policy is to establish a single, integrated framework for governing how Nasstar manages quality, information security, service management, business continuity, environmental responsibility, and regulatory compliance.

This policy ensures that all applicable legal, regulatory, contractual, and certification obligations are managed consistently, efficiently, and effectively through Nasstar's Integrated Management System (IMS).

2 Scope

This policy applies to:

- Applies to Nasstar, it's connected legal entities and its operating activities in the UK and overseas.
- All Nasstar employees, contractors, and third parties acting on Nasstar's behalf.
- All business units, services, systems, and locations.
- All activities within Nasstar's operational, technical, and corporate functions.

2.1 Compliance Obligations

Nasstar operates an Integrated Management System (IMS), embedded within its Management System, to support compliance with the following standards and frameworks:

International Standards & Certifications

- ISO 9001:2015 – Quality Management
- ISO 27001:2022 – Information Security Management

- ISO 14001:2015 – Environmental Management
- ISO 20000-1:2018 – IT Service Management
- ISO 22301:2019 – Business Continuity Management
- Cyber Essentials
- Cyber Essentials Plus
- PCI DSS v4.0

Regulatory and Sector Obligations

- Network and Information Systems (NIS) Regulations
- Ofcom General Conditions of Entitlement
- Telecoms Security Act (TSA)
- Public Services Network (PSN)
- Health and Social Care Network (HSCN)

The IMS provides a unified approach to managing these obligations through shared governance, risk management, controls, monitoring, and assurance activities.

3 Breach Management, Exceptions & Escalations

- Suspected or confirmed non-compliance must be reported promptly to compliance@nasstar.com
- Incidents are managed through defined incident and escalation processes.
- Corrective actions arising from Internal, External Audits or other formal means are to be identified, implemented, and tracked.
- Serious issues are escalated to Risk and Audit Committee and the Board as appropriate.

Exceptions to policies may only be made with formal and written approval. To make requests of exception please submit this request via email to compliance@nasstar.com detailing the rationale for the requested exception.

4 Policy Statement

Nasstar is committed to:

- Delivering high-quality, reliable, and secure services
- Protecting information, systems, and customer data
- Maintaining service resilience and continuity
- Meeting environmental responsibilities
- Complying with all applicable legal, regulatory, and contractual requirements
- Continually improving the effectiveness of the BMS and IMS

Nasstar is a leading provider of managed cloud, network, and communications services, supporting customers across critical national infrastructure, public sector, and regulated environments. Our reputation is built on delivering secure, resilient, high-quality services that our customers can trust.

To achieve this, Nasstar is committed to operating a robust Integrated Management System (IMS), which governs how we manage quality, security, service delivery, resilience, environmental responsibility, and regulatory compliance across the organisation.

We believe that best practice is defined by how our customers, regulators, partners, and other interested parties experience our services. The true measure of our effectiveness is our ability to consistently meet and where possible exceed their requirements and expectations, while operating ethically, responsibly, and sustainably.

In support of this commitment, Nasstar focuses on the following principles:

- **Quality & Service Excellence:** Delivering reliable, high-performing services through well-designed processes that ensure service availability, reliability, and the consistent achievement of contractual and service level commitments.
- **Security & Resilience:** Protecting the confidentiality, integrity, and availability of information, systems, and services. Security and resilience are embedded into our operations to safeguard customer data, maintain service continuity, and respond effectively to evolving cyber and operational threats.
- **Regulatory & Legal Compliance:** Meeting applicable legal, regulatory, contractual, and framework obligations, including those arising from telecommunications regulation, critical network services, and industry standards.
- **Environmental Responsibility:** Managing our environmental impacts responsibly by minimising the environmental footprint of our operations and technology, preventing pollution, and meeting applicable environmental obligations.
- **Continual Improvement:** Regularly reviewing performance against defined objectives to drive continual improvement, enhance operational effectiveness, and strengthen our management system.

The long-term success of Nasstar depends upon the success, security, trust, and sustainability of our customers and stakeholders.

By adopting a risk-based approach to the IMS, Nasstar ensures that risks and opportunities are identified, assessed, prioritised, and appropriately managed. This enables continuous monitoring and improvement of our people, processes, and technology, ensuring the IMS remains effective, proportionate, and aligned to our strategic objectives.

4.1 Management Commitment

Senior Management and the IMS governance structure are fully committed to the establishment, operation, maintenance, and continual improvement of the Integrated Management System.

The Risk and Compliance Team, supported by risk, process and asset owners across the business, is responsible for the effective management and oversight of the IMS. This includes ensuring that the IMS remains aligned with Nasstar's strategic direction, risk appetite, and regulatory obligations.

Management is committed to the following objectives:

- **Protecting Assets:** Ensuring the appropriate protection of information, systems, services, and physical assets, and compliance with applicable legal, regulatory, and contractual obligations.
- **Directing Business Activities:** Establishing, maintaining, and enforcing policies, standards, procedures, and guidelines that support consistent and controlled operations across Nasstar.
- **Meeting Interested Party Needs:** Understanding and meeting the requirements and expectations of customers, regulators, partners, suppliers, and employees.
- **Managing Risks and Opportunities:** Identifying, assessing, and managing risks and opportunities in a structured and proportionate manner, in line with Nasstar's risk appetite.
- **Providing Education and Awareness:** Ensuring that employees and relevant third parties are aware of their responsibilities and are appropriately trained to support the effective operation of the IMS.

- **Measuring Performance and Compliance:** Establishing metrics, monitoring activities, and assurance mechanisms to measure compliance, performance, and the effectiveness of the IMS, and to drive continual improvement.

4.2 Integrated Management System Objectives

Nasstar establishes and maintains a set of high-level Integrated Management System (IMS) objectives that provide a consistent direction for managing quality, information security, service management, business continuity, environmental responsibility, and regulatory compliance.

These objectives are aligned to Nasstar's strategic direction, risk appetite, and applicable ISO standards and regulatory obligations. They are reviewed periodically through management review to ensure they remain appropriate, effective, and relevant.

The core IMS objectives are:

- **Deliver Consistent, High-Quality Services:** Ensure the consistent delivery of professional, secure, resilient, and high-quality cloud, data, network, and security services across all operational locations, in line with quality and service management principles and contractual commitments.
- **Protect Information, Systems, and Data:** Protect the confidentiality, integrity, and availability of information, systems, and services through proportionate, risk-based information security and cyber resilience controls.
- **Maintain Service Resilience and Business Continuity:** Ensure critical services can be maintained and recovered within agreed tolerances through effective business continuity, incident management, and resilience planning.
- **Meet Legal, Regulatory, and Contractual Obligations:** Ensure ongoing compliance with all applicable legal, regulatory, contractual, and framework requirements through structured governance, monitoring, and assurance.
- **Drive Continual Improvement:** Continuously improve the effectiveness of the IMS by learning from performance monitoring, incidents, audits, feedback, and changes in risk, technology, regulation, and business strategy.

4.3 Monitoring, Reporting & Assurance

Nasstar operates a risk-based approach to managing its obligations.

- Risks are identified, assessed, and managed within defined risk appetite.
- The IMS controls are aligned to key operational, security, resilience, and regulatory risks.
- Risk assessments inform control selection, prioritisation, and improvement activities.
- Legal, regulatory, and contractual obligations are identified, documented, and maintained.
- Compliance requirements are mapped to policies, standards, and controls within the IMS.
- Changes in obligations are monitored and assessed for impact.
- Evidence of compliance is maintained and made available for audit and regulatory review.

Nasstar monitors the effectiveness of the IMS through:

- Management review activities
- Key performance and risk indicators
- Compliance monitoring and testing
- Internal and external audits

- Certification and regulatory assessments
- Findings are tracked, reported, and remediated in a timely manner

Nasstar ensures that all relevant employees and third parties receive training appropriate to their roles and responsibilities to support the effective operation of the Integrated Management System. Awareness of this policy, along with associated requirements, is maintained across the organisation through induction, ongoing communication, and targeted training activities. Training completion and competency are monitored to provide assurance that individuals understand and can fulfil their responsibilities in line with the IMS.

Nasstar is committed to the continual improvement of the Integrated Management System to ensure it remains effective, proportionate, and aligned to business and regulatory needs. Improvement activities are driven through management review, lessons learned from incidents, non-conformities and audits, feedback from customers and other stakeholders, and changes in risk, technology, regulation, and business strategy.

4.3.1 Objectives, Measurement, and OKR Framework

To support the effective implementation of the IMS objectives, Nasstar operates a structured framework for setting, monitoring, and reviewing measurable objectives using an Outcomes-focused approach.

High-level IMS objectives are translated into measurable targets through Objectives and Key Results (OKRs) or equivalent performance measures. This framework ensures that IMS objectives are:

- Measurable and outcome-focused
- Aligned to risk and compliance priorities
- Consistent with applicable ISO standards
- Reviewed regularly by management

IMS objectives define what Nasstar seeks to achieve in relation to quality, security, resilience, compliance, and continual improvement. Objectives are set at an organisational level and remain stable over time.

Key Results define how success is measured. They are specific, measurable, and time-bound outcomes that demonstrate progress towards each IMS objective. Key Results may cover areas such as service performance, customer satisfaction, risk reduction, compliance, training, or improvement activities.

Progress against IMS objectives and associated Key Results is monitored through management reporting and reviewed as part of formal management review activities. Where objectives are not being met, corrective actions are identified and tracked to completion.

This framework supports compliance with ISO standards' requirements for objective setting, performance evaluation, and continual improvement, while enabling a consistent and transparent approach to managing IMS performance.

5 Roles and Responsibilities

Board and Risk & Audit Committee

- Provide overall governance and strategic oversight of the IMS.
- Approve this policy and significant changes to the BMS.
- Ensure adequate resources are allocated to maintain compliance.

First Line – Doing the work	Second Line – Setting the rules and checking	Third Line – Independent assurance
Business Units, Process, Risk and Asset Owners: • Own and manage risks within their areas of responsibility. • Implement and comply with policies, standards, and procedures. • Maintain evidence of control operation.	**Risk & Compliance and Central Services** (i.e. People, IT & Security and Procurement etc.) • Define policies, standards, and control requirements. • Provide oversight, guidance, and challenge. • Monitor compliance and report on effectiveness.	**Internal Auditors and Risk & Audit Committee** • Provide independent assurance over the design and effectiveness of the IMS. • Report findings to senior management and the Board.

6 Policy Governance

This policy is to be reviewed on a minimum of an annual basis or in line with business or regulatory landscape changes.

All stakeholders under the scope of this policy are obligated to promptly report any breaches by emailing Compliance@nasstar.com

Definition of non-adherence includes, but is not limited to:

- Failure to follow any stated rule, procedure, or protocol outlined within this policy.
- Deliberate circumvention of control measures, processes, or systems established to support this policy.
- Negligent actions or omissions that result in a breach or violation of the policy's intent or requirements.

Any confirmed instance of non-adherence to this policy, regardless of whether it results in immediate loss or harm to the Company, will be treated as a serious matter of misconduct and may result in the trigger of the Nasstar's formal Disciplinary Procedure.

7 Definitions & Acronyms

- **Integrated Management System (IMS)**
  The overarching framework through which Nasstar manages quality, information security, service management, business continuity, environmental responsibilities, and compliance in an integrated and coordinated manner.
- **Management System**
  The collection of policies, standards, processes, procedures, and controls that support the operation and continual improvement of the IMS.
- **Interested Parties**
  Individuals or organisations that can affect, be affected by, or perceive themselves to be affected by Nasstar's activities, services, or decisions, including customers, regulators, partners, suppliers, and employees.
- **Risk-Based Approach**
  A structured method of identifying, assessing, and managing risks and opportunities in line with Nasstar's risk appetite to prioritise controls and resources.

- **Compliance Obligations**
  Legal, regulatory, contractual, and framework requirements that Nasstar is required to comply with, including those arising from legislation, regulation, certification schemes, and customer agreements.
- **Continual Improvement**
  Ongoing activities undertaken to enhance the effectiveness, suitability, and adequacy of the IMS through monitoring, review, and corrective actions.
- **Non-conformity**
  A failure to meet a requirement of the IMS, an applicable standard, regulation, policy, or contractual obligation.
- IMS – Integrated Management System
- ISMS – Information Security Management System
- BCMS – Business Continuity Management System
- ITSM – IT Service Management
- OKR – Objectives and Key Results
- ISO – International Organization for Standardization
- NIS – Network and Information Systems Regulations
- PSN – Public Services Network
- HSCN – Health and Social Care Network
- PCI DSS – Payment Card Industry Data Security Standard