Governance, Risk and Compliance Whitepaper

SUMMARY

Tre & Hallon (Hi3G Access AB) is committed to operating with the highest standards of integrity, security and sustainability. This whitepaper provides an overview of our comprehensive governance framework, built on **14 governing policies** that guide everything we do, from ethical conduct and data protection to information security and environmental responsibility.

As part of the CK Hutchison Group (60%) and Investor AB (40%), Tre operates with robust oversight while maintaining the challenger spirit that defines our brand.

Disclaimer

This whitepaper is created for guidance purposes only regarding Hi3G Access AB. It does not constitute a legally binding commitment. Any binding obligations between Hi3G and any other party must be set out in a written agreement in accordance with Hi3G's general terms and conditions.

Table of contents

Governance, Risk and Compliance Whitepaper 0
Summary 1
Governance Framework 3
Information Security 4
Data Protection & Privacy 6
Anti-Corruption & Business Ethics 8
Sustainability & ESG 9
Human Resources & People 10
Supplier & Third-Party Management 11
FAQ 12

GOVERNANCE FRAMEWORK

Three Lines of Defense

Our Internal Governance & Control Policy (v3.0) establishes a structured governance model:

- **First line:** Business operations own and manage risks in their respective areas
- **Second line:** GRC (Governance, Risk & Compliance) provides oversight, frameworks and independent challenge
- **Third line:** Internal audit provides independent assurance

Risk Management

The Risk Policy (v3.1) defines a comprehensive risk framework with:

- Management-defined risk appetite reviewed annually
- Annual risk assessment cycle covering all material risks
- RACI model for clear accountability across the organization
- Structured escalation paths for risk events and incidents

Insurance

Hi3G maintains a comprehensive insurance programme designed to protect the company, its operations and its stakeholders. Our coverage includes standard corporate insurance such as liability and product liability insurance, property and business interruption insurance, and dedicated cyber insurance. The programme is reviewed annually to ensure that it remains aligned with our risk profile, contractual obligations and industry practice.

Board & Leadership Accountability

The Board, CEO and CxO/VP levels have clearly defined responsibilities for governance, compliance and risk management. The CEO decides all governing policies.

INFORMATION SECURITY

ISMS Framework

Information security is a fundamental component of our operations and a key element in the trust our clients place in us. We manage information security thorugh a structured Information Security Management System (ISMS) aligned with the principles and control framework of ISO 27001, the NIS2 directive and national telecom regulations (PTSFS 2022:11). Our ISMS provides a systematic approach to identifying, managing, and reducing risks related to the confidentiality, integrity, availability, and traceability of information.

Control framework

Our security controls are implemented across four core domains in accordance with the standard ISO27001 to provide comprehensive protection throughout the organization:

- **Organizational controls**
  This includes clearly defined policies, risk management processes, asset management, supplier security requirements, incident management procedures, and business continuity management. These controls ensure that the information security work is risk-based, and that security responsibilities are embedded into organizational processes.
- **People controls**
  Employees and contractors play a critical role in maintaining information security. We implement people focused controls such as background screening (e.g. criminal and financial history), terms and conditions of employment, security awareness training, role-based access management, and clearly defined responsibilities for protecting information. Continuous training helps ensure that our personnel understand security risks and their role in mitigating them.
- **Physical controls**
  Physical security measures protect facilities, infrastructure and hardware from unauthorized access, damage, or disruption. Measures include controlled access to sensitive areas, visitor management, environmental protections, secure equipment handling, and facility monitoring designed to protect systems and the information they process.
- **Technological controls**
  Technical security measures protect systems, networks, and data against unauthorized access, misuse, and cyber threats. These controls include among others identity and access management, backup management, secure development, monitoring and logging, vulnerability management, network security, and malware protection.

Structured governance and continuous improvements

Our information security program is built on a governance model that integrates security into business processes, decision-making, and operational activities. We have a set of defined and established policies, guidelines, and procedures to ensure that security practices are consistently applies across the organization. Examples of policies and procedures in our Policy framework include:

- Information Security Policy
- Acceptable Use Policy
- Information Security Risk Management Instruction
- Security Guidelines
- Incident Management
- Access Management

- Asset Management
- Supplier Security Instruction
- Business Continuity Plan
- ISMS Instruction

To ensure that security measures remain effective and relevant in a constantly evolving threat landscape, we work with continuous improvements. Key Performance Indicators (KPIs) are used to measure the effectiveness of security controls, monitor compliance with internal policies, and identify areas for improvement. Regular risk assessments, internal reviews, and management oversight ensure that the ISMS evolves alongside the business needs, technological changes, and emerging threats.

Key Security Measures

- **Access control:** Principle of least privilege with regular auditing of accounts, roles and permissions.
- **Multi-factor authentication:** Should be activated where possible.
- **Encryption:** Cryptographic methods of proven strength.
- **Network security:** Firewalls, IDS/IPS, network segregation, anti-spoofing measures, WAF for external web traffic.
- **Vulnerability management:** Processes to identify, evaluate, track, manage and remediate vulnerabilities.
- **Malware protection:** Detection, prevention and recovery controls combined with user awareness training.
- **Secure development:** Secure coding practices, security testing throughout the SDLC, risk assessment during system acquisition.

Incident Management & Business Continuity

- Defined incident classification levels and escalation paths
- Ability to report significant incidents within **24 hours** (NIS2) and **72 hours** (GDPR)
- Crisis management team with structured response procedures
- Business continuity planning with redundancy for critical network components
- Disaster recovery plans tested and updated regularly

Monitoring & Logging

- Monitoring mechanisms to detect anomalous behaviour and potential security incidents
- Audit trails and traceability for applicable systems
- Backup management with logs retained per business and legal requirements, stored separately from production

DATA PROTECTION & PRIVACY

GDPR Compliance

The Data Protection Policy (v1.0) governs all personal data processing where Tre is data controller or data processor. It ensures compliance with the GDPR and the CK Hutchison Group Policy on Personal Data Governance.

Privacy Organization
Tre maintains a dedicated privacy organization:

- **Data Protection Officer (DPO)** operating as a second-line control function within GRC
- **Team Privacy** consisting of *Legal Counsels* and *Privacy Specialists* for legal guidance, operational privacy management and incident management for breach response.

The privacy team supports the organization when processing personal data or implementing new systems, and works closely with the Information security team, regulatory team, legal team and costumer relations team to ensure that the GDPR aligns with other areas of law and/or rights and requirement.

Core principles applied:

Privacy works to ensure GDPR compliance within the organisation, including but not limited to, defining legal grounds, documenting purposes and data protection risks, processing records and uphold data subjects' rights. The GDPR core principles are considered through all processing activities:

- Lawfulness, fairness and transparency
- Purpose limitation and data minimization
- Accuracy, storage limitation
- Integrity and confidentiality

As a telecommunications provider, Tre also complies with the Swedish Electronic Communications Act (LEK). LEK introduces additional, sector-specific requirements concerning confidentiality of communications, handling of traffic and location data, network security, and obligations toward law enforcement authorities. These requirements are integrated into operational processes and apply alongside GDPR.

Risk & Compliance Management
Privacy considerations are embedded into all processing activities from the outset, following the GDPR principles of *privacy by design and by default*. *Data Protection Impact Assessments (DPIAs)* are performed where required, ensuring risks are identified and mitigated. Employees receive an introduction to basic privacy-related considerations during the onboarding process, as well as yearly mandatory *data protection education.*

Security measures and international transfers
Tre applies appropriate technical and organisational measures, including yearly training for employees, access management, retention, encryption, and incident response. The Privacy team operates in accordance with Information Security's standards and collaborates with the ISO function on activities that require heightened security and formal security risk evaluations, for example when conducting DPIAs.

We avoid processing outside the EU/EEA, if the country does not have an adequacy decision. Where processing's outside the EU/EEA occur, appropriate safeguards must be implemented, including Standard Contractual Clauses (SCCs) and a thorough Transfer Impact Assessments (TIA).

ANTI-CORRUPTION & BUSINESS ETHICS

Zero Tolerance

The Anti-Corruption Policy (v2.1) establishes a zero-tolerance stance on:

- Bribery and corruption
- Fraud and money laundering
- Facilitation payments
- Third-party corrupt behaviour

The policy is decided by the CEO. Leadership leads by example.

Code of Conduct

The Code of Conduct (v1.4) guides all employees on ethical behaviour, fostering a culture of **Challengers, Champions and Buddies**. It covers:

- Zero tolerance for discrimination and harassment
- Rules on gifts, hospitality and conflicts of interest
- Confidentiality obligations
- Applicable to all employees and representatives

Business Partner Standards

The Code of Conduct for Business Partners (v2026) is based on:

- UN Global Compact principles
- OECD Guidelines for Multinational Enterprises
- ILO Core Conventions

It requires human rights and fair labor compliance, anti-corruption standards, environmental responsibility, and generally grants Tre the right to audit and verify compliance.

Whistleblowing

Tre provides established reporting channels:

- **WhistleB** (Whistleblowing Centre) https://report.whistleb.com/en/tre

The whistleblowing function is available to both employees and certain external parties.

Competition Compliance

The Competition Policy (v2.2) ensures fair competition in line with antitrust law, covering:

- No anti-competitive agreements
- Rules for competitor contact and information exchange
- Dawn raid preparedness procedures
- Sanctions awareness and prevention

SUSTAINABILITY & ESG

ESG Strategy

The Sustainability Policy (v2.1) integrates Environmental, Social and Governance dimensions across the entire business. Tre is a member of the **UN Global Compact** and committed to the **Science Based Targets initiative (SBTi)**.

Our SBTi-Aligned Climate Targets

Target	Timeline
Scope 1 & 2 emissions reduction	**70% by 2030** (base year 2022)
Scope 3 emissions reduction	**42% by 2030** (base year 2022)
Net-zero emissions	**2040**
Renewable electricity	**100%** target

Emissions are measured and reported according to the **Greenhouse Gas Protocol** standard.

Environmental Commitments

- Climate impact reduction
- Energy efficiency
- Contribute to a circular economy

Social Responsibility

- Diversity, inclusion and equal opportunities as strategic priorities (own workforce)
- Human rights and fair labor throughout the value chain
- Zero tolerance for forced and child labor throughout the value chain
- Occupational health and safety compliance throughout the value chain
- Freedom of association and collective bargaining respected throughout the value chain

Governance

- ESG-linked executive compensation
- Annual sustainability report per applicable legislation
- Board, CEO and Senior management oversight of ESG performance
- Performance tracked against established targets and KPIs

See section ”ANTI-CORRUPTION & BUSINESS ETHICS”.

HUMAN RESOURCES & PEOPLE

Background Screening

The HR Policy (v1.2, section 3.5.2) requires background checks on all new hires and internal recruitments involving personnel responsibility. Consultants must meet at least the same qualifications as employees.

Security Awareness Training

- All employees receive adequate security awareness training regularly
- Security culture improvement is a core ISMS objective

Work Environment

- Safe and healthy work environment in compliance with applicable legislation
- Physical and psychological safety addressed
- Zero tolerance for harassment, bullying and discrimination
- Strict alcohol/narcotics policy
- Workplace conflict of interest management

Diversity & Inclusion

- Diversity positioned as a strategic strength
- Equal opportunities promoted across the organization
- Fair compensation and pension framework

Employee Rights

- Compliance with labor law and collective agreements
- Freedom of association and collective bargaining respected

SUPPLIER & THIRD-PARTY MANAGEMENT

Sourcing Governance

The Sourcing Policy (v1.4) structures procurement from planning through contract signing:

- Supplier evaluation and risk management
- Purchase order process governance

Security Requirements

- Security requirements specified in written agreements before granting access
- Code of Conduct for Business Partners is a requirement in most agreements
- Vetting and compliance monitoring of sub-contractors

Please refer to tre.se/gpc for more information.

Audit Rights

In general, Tre maintains full audit rights over suppliers, enabled by:

- Code of Conduct for Business Partners audit clauses
- Sourcing Policy audit provisions
- Internal Governance & Control oversight

FAQ

The following questions and answers address common due diligence and supplier assessment inquiries, organized by topic area and grounded in our 14 governing policies.

Information Security

Question	Answer
Does Tre have a security certification or certified management system (e.g. ISO 27001)?	Tre is not ISO 27001 certified. However, our Information Security Policy (v1.2) establishes an ISMS structured and aligned with the ISO 27001:2022 framework. The policy maps to ISO 27001 Clause 5.2, NIS2 Article 21, and national telecom regulations (PTSFS 2022:11). Our security framework follows the Plan-Do-Check-Act cycle and is subject to regular internal audits.
Does Tre have an appointed security responsible with defined roles?	Yes. Our Information Security Policy defines clear roles: the CEO holds ultimate responsibility, CxO/VPs ensure compliance within their areas, and a dedicated Information Security Officer oversees the ISMS. Security Officers/Managers handle operational security, and all Hi3G personnel are responsible for adhering to security policies.
Does Tre have an established ISMS with IT and information security policies?	Yes. Tre maintains a comprehensive ISMS governed by two complementary policies: the Information Security Policy (strategic framework, objectives and roles) and the Security Policies document (detailed organizational, people, physical and technological controls). Both are structured according to and aligned with the ISO 27001:2022 framework, though Tre is not formally certified.
Does Tre perform regular risk analysis considering confidentiality, integrity and availability?	Yes. Our Risk Policy (v3.1) mandates annual risk assessments with a defined risk appetite set by the board. The Security Policies require information security risk management that considers internal and external threats to confidentiality, integrity and availability. We use a RACI model for clear accountability.
Does Tre perform vulnerability management and security testing?	Yes. Our Security Policies (v1.2) require processes to identify, evaluate, track, manage and remediate vulnerabilities in a timely manner (section 11.6). The Secure Development section (11.10) mandates security testing throughout the software development lifecycle.
Does Tre have procedures for data encryption (in-transit and at-rest)?	Yes. The Security Policies include a cryptography section (11.7) requiring cryptographic methods of proven strength to protect information assets. This covers cryptographic key protection, key management, key revocation, and Public Key Infrastructure using X.509 standards.
Does Tre have established network security controls to prevent and detect cyberattacks?	Yes. Our Security Policies cover network security including firewall implementation, IDS/IPS capabilities, network segregation, anti-spoofing measures and Web Application Firewalls (WAF) for external web traffic.
Does Tre have multi-factor authentication (MFA) implemented?	The Security Policies (section 8.3.3) state that systems should be integrated with centralized identity management (Active Directory) where possible, and that multi-factor authentication should be activated where possible. Access control is based on the principle of least privilege.
Does Tre have an established incident management policy and procedure?	Yes. The Security Policies include a Security Incident Management section with defined roles, procedures, classification levels and escalation paths. We are able to report significant incidents within 24 hours as required by NIS2 and GDPR.
Does Tre have a Business Continuity Plan and Disaster Recovery Plan?	Yes. Our Security Policies address business continuity with redundancy requirements for critical network components. The Risk Policy framework covers business continuity

	planning, and BCPs and DRPs are tested and updated regularly.
Does Tre have anti-malware/EDR software deployed on all systems?	Yes. The Security Policies (section 11.4) require detection, prevention and recovery controls to protect against malware, combined with appropriate user awareness training.
Does Tre have log retention policies and audit logging in place?	Yes. Our Security Policies (section 11.3) require monitoring mechanisms to detect anomalous behaviour and potential security incidents. Logs must establish traceability and audit trails for applicable systems.
Does Tre have physical security controls for sensitive facilities?	Yes. The Security Policies cover physical security perimeters, protection against physical and environmental threats, and equipment security. Only authorized parties have physical access to sensitive facilities.
Does Tre have a secure development lifecycle process?	Yes. Our Security Policies (section 11.10) require secure coding practices following industry standards, security testing throughout the development lifecycle, and risk assessment during system acquisition and development.

Data Protection & Privacy

Question	**Answer**
Does Tre comply with the GDPR and applicable data protection legislation?	Yes. Our Data Protection Policy (v1.0) governs all personal data processing. It ensures compliance with the GDPR and is complemented by the CK Hutchison Group Policy on Personal Data Governance. Tre has a dedicated privacy organization with a DPO, privacy specialists and legal counsel.
Does Tre have a formal data protection/privacy policy in place?	Yes. The Hi3G Data Protection Policy (v1.0) covers all processing where Tre is data controller or data processor. It defines fundamental principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity & confidentiality.
Has Tre appointed a Data Protection Officer (DPO)?	Yes. Our Data Protection Policy establishes a comprehensive privacy organization including a DPO, Team Privacy, Privacy Specialists, Legal Counsel and Incident Managers. The DPO operates as a second-line control function within GRC.
Does Tre maintain a Record of Processing Activities (ROPA)?	Yes. As part of GDPR compliance, our Data Protection Policy requires documentation of all processing activities. The privacy organization maintains records and conducts regular reviews to ensure compliance.
Does Tre have processes to handle personal data breaches within 24 hours?	Yes. Our Data Protection Policy includes incident management procedures with designated incident managers. We can identify, report, manage and resolve personal data breaches within required timeframes (24h for NIS2, 72h for GDPR).
Do Tre's services comply with data protection by design and by default?	Yes. The Data Protection Policy mandates that privacy considerations are embedded into all processing activities from the outset, following the GDPR principles of privacy by design and by default.
Does Tre only process personal data inside the EU/EEA?	Our Data Protection Policy aligns with CK Hutchison Group standards and the GDPR requirements for international transfers. Processings outside the EU/EEA are carefully evaluated. If there is not an adequacy decision in place, appropriate safeguards such as Standard Contracual Clauses (SCC) must be considered before the transfer takes place. Transfer Impact Assessments are made for all processing.

Anti-Bribery & Anti-Corruption

Question	Answer
Does Tre have an Anti-Bribery and Anti-Corruption (ABAC) policy?	Yes. Our Anti-Corruption Policy (v2.1) establishes a zero-tolerance stance on bribery, fraud, money laundering and corrupt behaviour.
Does Tre's Code of Conduct include rules against bribery and corruption?	Yes. Our Code of Conduct (v1.4) explicitly addresses anti-corruption, gifts & hospitality, and conflicts of interest. It is complemented by the dedicated Anti-Corruption Policy.
Does Tre provide regular anti-bribery and corruption training?	Yes. The Anti-Corruption Policy mandates continuous training on ethics and anti-corruption for all employees. Leadership is expected to lead by example.
Does Tre have a whistleblowing or reporting channel?	Yes. Tre has established whistleblowing systems: WhistleB. Deviations and other incidents can also be reported through Tre's incident reporting system or directly to the Compliance Officer.
Does Tre have policies on gifts, hospitality and entertainment?	Yes. Both the Anti-Corruption Policy and Code of Conduct contain strict rules on giving and receiving gifts, hospitality and entertainment with detailed thresholds and approval requirements.
Does Tre prohibit facilitation payments?	Yes. The Anti-Corruption Policy explicitly covers facilitation payments as part of its zero-tolerance approach to all forms of corruption.
Is Tre's senior management committed to zero-tolerance on corruption?	Yes. The Anti-Corruption Policy is decided by the CEO. Leadership shall lead by example following our anti-corruption strategy "Champions don't cheat"
Does Tre conduct due diligence on third parties and intermediaries?	Yes. Our Sourcing Policy (v1.4) and Code of Conduct for Business Partners require supplier evaluation, risk management and compliance verification.

ESG & Sustainability

Question	Answer
Does Tre have a sustainability or ESG strategy?	Yes. Our Sustainability Policy (v2.1) integrates ESG across the entire business. Tre is committed to SBTi and is a member of the UN Global Compact.
Does Tre publish ESG results in an annual report?	Yes. Tre prepares an annual sustainability report in accordance with applicable legislation. Performance is tracked against established targets and KPIs.
Does Tre have a code of conduct and policies supporting responsible business?	Yes. Tre maintains a Code of Conduct (v1.4) for employees and a Code of Conduct for Business Partners (v2026) based on UN Global Compact, OECD Guidelines and ILO Core Conventions.
Does Tre comply with human rights outlined in the Code of Conduct?	Yes. Our Code of Conduct for Business Partners explicitly requires adherence to the UN Declaration on Human Rights, fair labor practices and ILO Core Conventions.
Does Tre ensure no forced or child labor in its operations or supply chain?	Yes. The Code of Conduct for Business Partners explicitly prohibits forced and child labor throughout operations and supply chains.
Does Tre comply with occupational health and safety legislation?	Yes. Our HR Policy (v1.2) mandates a safe and healthy work environment in compliance with applicable legislation.
Is Tre monitoring and disclosing Scope 1, 2 and 3 GHG emissions?	Yes. Tre has SBTi-approved targets: reducing Scope 1 & 2 by 70% and Scope 3 by 42% by 2030 (base year 2022), with net-zero by 2040. Emissions follow the Greenhouse Gas Protocol.

Does Tre have an environmental/sustainability policy?	Yes. The Sustainability Policy (v2.1) covers climate impact reduction, energy efficiency, circular economy practices, and responsible sourcing.
Does Tre have a sustainability screening for its suppliers?	Yes. The Sourcing Policy requires supplier evaluation including sustainability criteria. Tre reserves the right to audit and verify compliance.
Does Tre ensure discrimination is not tolerated?	Yes. Both the Code of Conduct and HR Policy establish zero tolerance for discrimination, harassment and bullying.

Human Resources & People

Question	Answer
Does Tre perform background screening of employees and contractors?	Yes. Our HR Policy (v1.2, section 3.5.2) requires background checks on all new hires and internal recruitments involving personnel responsibility. Consultants must meet at least the same qualifications as employees.
Does Tre provide information security awareness training?	Yes. The Security Policies require all employees to receive adequate security awareness training regularly. Annual obligatory training is managed by HR.
Does Tre recognize employees' rights to freedom of association and collective bargaining?	Yes. The HR Policy ensures compliance with labor law and collective agreements. The Code of Conduct for Business Partners explicitly requires respect for these rights.
Does Tre have policies addressing diversity and inclusion?	Yes. The HR Policy promotes equal opportunities. The Code of Conduct reinforces that diversity and different perspectives are strengths.
Does Tre have policies on workplace safety and well-being?	Yes. The HR Policy covers work environment including physical and psychological safety, harassment, bullying, alcohol/narcotics policy, and workplace conflicts of interest.

AI Governance

Question	Answer
Does Tre have governance procedures for responsible AI use?	Yes. Tre's policy framework — including the Internal Governance & Control Policy, Risk Policy and Security Policies — provides the foundation for responsible technology use, including AI.
How does Tre handle AI systems that process personal data?	Any AI system processing personal data falls under Tre's Data Protection Policy, requiring GDPR compliance, DPIAs, and adherence to data minimization and purpose limitation principles.
Does Tre assess AI systems under the EU AI Act?	Tre's risk-based approach (Risk Policy v3.1) and compliance framework provide the structure for assessing AI systems against regulatory requirements, including the EU AI Act.
How does Tre ensure data ownership and control with AI suppliers?	The Sourcing Policy and Security Policies require contractual clauses ensuring Tre retains ownership of its data. Suppliers must agree to return and delete data upon service termination.

Supplier & Third-Party Management

Question	Answer
Does Tre specify security requirements in agreements with suppliers?	Yes. The Sourcing Policy (v1.4) structures procurement with mandatory security and compliance requirements. The Code

	of Conduct for Business Partners is integral to all agreements.
Does Tre perform security vetting of sub-contractors?	Yes. Our Security Policies and Sourcing Policy require vetting and compliance monitoring of sub-contractors. Sub-contractors must meet the same standards as primary suppliers.
Does Tre have full audit rights over its suppliers?	Yes. The Code of Conduct for Business Partners grants Tre the right to audit and verify compliance. The Sourcing Policy includes audit rights clauses.
Does Tre ensure sub-contractors are within the EU/EEA?	Where suppliers operate outside the EU/EEA, additional safeguards including SCCs, data localization and enhanced due diligence are required.

Credit & Financial Controls

Question	**Answer**
Does Tre have financial controls to detect suspicious payments?	Yes. The Anti-Corruption Policy covers financial controls and monitoring. The Credit & Collection Policy (v1.0) governs credit assessment and monitoring.
Does Tre conduct due diligence on payment intermediaries?	Yes. The Anti-Corruption Policy requires due diligence on agents, consultants and intermediaries. The Sourcing Policy mandates evaluation before contracting.