Environment and Sustainability Framework

for Access and Asset Protection

Contents

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

1. Introduction

The environment and sustainability framework for access control-based solutions involves addressing the technology's environmental, social, and governance (ESG) aspects while ensuring the framework is actionable and aligns with organisational goals.

ESG stands for **Environmental, Social, and Governance**. It is a set of criteria used to evaluate an organisation's performance and practices in these three key areas:

Environmental - This aspect examines how a company's operations impact the environment. It includes factors like energy consumption, carbon footprint, waste management, resource conservation, and efforts toward sustainability and environmental stewardship.

Social -The social criterion assesses how a company manages relationships with employees, suppliers, customers, and the communities where it operates. It covers work practices, employee health and safety, diversity and inclusion, human rights, consumer protection, and community engagement.

Governance - Governance involves the company's leadership, executive pay, audits, internal controls, shareholder rights, and transparency. It evaluates how a company is governed and whether it adheres to laws, regulations, and ethical standards.

2. Purpose

The purpose of the sustainability framework is to guide the integration of environmentally friendly practices into access control solutions, making them more energy-efficient and resource-conscious. This is important to the organisation because it reduces environmental impact, enhances corporate social responsibility, and can lead to cost savings through improved efficiency and compliance with environmental regulations.

3. UK and EU regulations and standards that are applicable

A list of environmental and sustainability standards applicable to access control solutions throughout their lifecycle from manufacturing through installation to end-of-life disposal and recycling.

3.1. Compliance restrictions of hazardous substances in electronic products to meet environment and safety standards

RoHS Directive (2011/65/EU and Amendment (EU) 2015/863) **–** The application restricts the use of certain hazardous substances in electrical and electronic equipment (EEE). Manufacturers must ensure that devices do not contain prohibited levels of hazardous materials like lead, mercury, cadmium, hexavalent chromium, and specific phthalates.

UK RoHS Regulations (Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012) **-** The UK's implementation of RoHS post-Brexit. Similar to the EU RoHS, UK manufacturers and importers must comply with substance restrictions for products placed on the UK market.

REACH Regulation (EC No 1907/2006) **-** Registration, Evaluation, Authorisation, and restriction of chemicals in the EU. Manufacturers must identify and manage risks linked to substances used in their products, ensuring safe handling throughout the lifecycle.

UK REACH Regulations (UK REACH) - Post-Brexit UK version of the REACH regulation. Similar obligations as EU REACH for substances used in access control products within the UK market.

Environment Act 2021 (UK) **-** Introduces new environmental policies and legally binding targets in the UK. Manufacturers and installers need to comply with updated environmental standards and reporting requirements.

BS EN ISO 14001:2015 - UK adoption of the international standard for Environmental Management Systems (EMS). Organisations can implement EMS to reduce environmental impacts during manufacturing and installation process.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

BS EN IEC 63000:2018 - Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances. Supports compliance with RoHS requirements.

BS EN IEC 62430:2019 - Environmentally conscious design for electrical and electronic products. Guides the integration of environmental considerations into product design.

EN 50581 (Superseded by EN IEC 63000) - Provided technical documentation for RoHS compliance. Previously used for RoHS technical documentation; replaced by EN IEC 63000.

3.2. Governs the use and disposal of batteries within access control devices

Batteries and Accumulators (Placing on the Market) Regulations 2008 Applicability **-** UK regulations on batteries and accumulators.

3.3. Encourages the design of access control systems that are repairable, extending product lifespan

BS 8001:2017 Applicability - UK standard providing a framework for implementing circular economy principles guide.

BS EN ISO 14040/14044 - Standards for Life Cycle Assessment (LCA). Manufacturers can assess the environmental impacts of their products throughout their lifecycle.

UK Government's "Right to Repair" Legislation (2021) Applicability **-** Requires manufacturers to make spare parts available to consumers and professional repairers.

3.4. Guides organisations in designing business models and products that minimize waste

UK Waste Regulations (Waste Regulations 2011) Applicability - Implements the EU Waste Framework Directive in the UK.

Waste Framework Directive (2008/98/EC) - Sets the basic concepts and definitions related to waste management, recycling, and recovery within the EU. Influences waste management practices for end-of-life of equipment.

3.5. Influences how waste from access control devices is managed and recycled

Climate Change Act 2008 (UK) Applicability **-** Sets legally binding targets for the UK to reduce greenhouse gas emissions.

EU Taxonomy Regulation (Regulation (EU) 2020/852) Applicability **-** Establishes criteria to determine whether an economic activity is environmentally sustainable.

Circular Economy Action Plan (European Green Deal) - Aims to make sustainable products the norm in the EU. Encourages the design of devices for durability, repairability, and recyclability.

WEEE Directive (2012/19/EU) **-** Addresses the collection, treatment, recycling, and disposal of electronic waste. Producers are responsible for financing the collection and recycling of end-of-life access control devices.

UK WEEE Regulations (Waste Electrical and Electronic Equipment Regulations 2013) - The UK's implementation of the WEEE Directive. Obligates producers in the UK to register and finance the treatment and recycling of waste access control equipment.

3.6. Influences investment and development in sustainable access control technologies

BS EN ISO 50001:2018 Applicability - UK adoption of the international standard for Energy Management Systems.

Eco-design Directive (2009/125/EC) - Establishes a framework for setting eco-design requirements for energy-related products. Manufacturers must design access control systems that meet energy efficiency and environmental criteria.

UK Eco-design for Energy-Related Products and Energy Information Regulations 2021 **-** UK's implementation of ecodesign requirements post-Brexit. Control equipment must comply with UK-specific energy efficiency standards.

3.7. Organisations procuring access control solutions can ensure they select environmentally responsible products

BS ISO 20400:2017 - Sustainable Procurement Applicability - Provides guidance on integrating sustainability into procurement processes.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

3.8. While focused on data privacy, it affects the design and operation of access control systems that process personal data.

Data Protection Act 2018 (UK GDPR) - Regulates data protection and privacy in the UK.

EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Applicability - Regulates data protection and privacy in the EU.

3.9. Manufacturers must take responsibility for the packaging used with access control products

Energy Labelling Regulation (EU) 2017/1369 Applicability - Provides a framework for energy labelling of products to inform consumers.

Producer Responsibility Obligations (Packaging Waste) Regulations 2007 (as amended) - regulations on packaging waste management.

3.10. Application Across the Lifecycle

Adhering to key environmental and safety guidelines throughout an application's lifecycle, from manufacturing through installation to end-of-life disposal and recycling, ensures responsible material selection, energy-efficient installation, and eco-friendly disposal or recycling practices. Focusing on sustainability at each stage helps minimise environmental impact and supports long-term environmental stewardship.

The three applications across the lifecycle are:

- Manufacturing
  - **Compliance with RoHS and REACH -** Ensure restricted substances are not used.
  - **Environmental Management Systems -** Implement **BS EN ISO 14001** and **BS EN ISO 50001** to manage environmental impacts and energy use.
  - **Eco-design Principles:** Apply **BS EN IEC 62430** and the **Eco-design Directive** to create sustainable products.
  - **Circular Economy -** Use **BS 8001** to integrate circular economy principles.
- Installation
  - **Sustainable Procurement -** Follow **BS ISO 20400** to select environmentally friendly products and services.
  - **Energy Efficiency -** Ensure installation practices optimize energy use, supporting **Climate Change Act 2008** goals.
- End-of-Life Disposal and Recycling
  - **WEEE Compliance -** Adhere to the **WEEE Directive** and **UK WEEE Regulations** for proper disposal and recycling.
  - **Packaging Waste Management -** Comply with **Producer Responsibility Obligations** for packaging materials.
  - **Batteries Disposal -** Follow the **Batteries and Accumulators Regulations** for battery recycling.

4. Recommendations for Organisations

By conducting Life Cycle Assessments (LCA) in utilising BS EN ISO 14040/14044 to evaluate environmental impacts from cradle to grave, consider the implementation of sustainable design **to** integrate environmental considerations early in the product development process using BS EN IEC 62430. Also consider obtaining certifications for environmental management like BS EN ISO 14001 and looking at energy efficiency like BS EN ISO 50001 to demonstrate commitment to sustainability.

Promote Repairability to align with the 'Right to Repair' legislation by designing products that are easier to repair and maintain.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

Note: Compliance with these UK and EU-specific standards and regulations not only helps reduce environmental impact but also ensures legal compliance, enhances corporate reputation, and meets customer demand for sustainable products.

By defining the scope, to include the access control solutions covered (e.g. physical access, digital access, biometric systems), you define your sustainability framework, which covers all access control solutions utilised by the organisation.

This includes:

- **Physical Access Systems -** Such as keycards, turnstiles, and security doors, and RFID card access.
- **Digital Access Controls -** Including password protocols, multi-factor authentication, and secure login systems.
- **Biometric Systems -** Like fingerprint scanners, facial recognition, and iris scanning technologies.

The framework applies to both hardware and software components, ensuring that sustainable practices are implemented across all types of access control technologies in use, such as reducing carbon footprint, enhancing security, and promoting responsible sourcing, etc, to a more descriptive set of defined objectives listed below.

The sustainability framework aims to achieve the following objectives:

- **Reduce Carbon Footprint -** Implement energy-efficient access control systems to minimize energy consumption and lower greenhouse gas emissions.
- **Enhance Security Responsibly -** Maintain high levels of security while integrating environmentally friendly practices.
- **Promote Responsible Sourcing -** Ensure that all materials and components used in access control solutions are ethically sourced and have minimal environmental impact.
- **Fire safety -** Making sure that products are environmentally friendly that don't degrade fire safety.
- **Minimize Electronic Waste -** Extend the lifecycle of equipment through upgradability and recycling programs to reduce e-waste.
- **Compliance with Environmental Regulations -** Adhere to all relevant environmental laws and standards to ensure responsible operations.

These objectives support the organisation's commitment to environmental stewardship while maintaining effective access control solutions.

5. Sustainability Principles

Sustainability responsibilities regarding environmental responsibility focus on reducing the ecological impact of access control systems, from production to disposal. This involves using eco-friendly materials, implementing energy efficient operations, designing durable and upgradable systems to extend their lifespan, and ensuring responsible disposal or recycling. By integrating these practices, the Organisation reduces its ecological footprint while maintaining effective security solutions.

5.1. Energy Efficiency

Emphasize the use of energy-efficient devices and systems in access control solutions. This involves selecting hardware with low power consumption, utilising power-saving modes, and implementing software optimisations to reduce energy usage. Consider integrating technologies like LED indicators and energy-efficient processors. Additionally, explore the use of renewable energy sources, such as solar power for standalone units. Focusing on energy efficiency reduces operational costs and minimises environmental impact while maintaining effective security.

5.2. Materials - Promote the use of sustainable, recyclable, and non-toxic materials

Promote the use of sustainable, recyclable, and non-toxic materials in access control systems. This involves selecting components made from recycled or renewable resources and avoiding hazardous substances like lead or mercury (Please refer back to sub-section 3.1 with regards to compliance in restrictions of hazardous substances in electronic products to meet environment and safety standards). Design products for easy disassembly to facilitate recycling at the end of their life cycle. Prioritise suppliers who provide materials certified for environmental friendliness and responsible sourcing. By focusing on sustainable materials, the organisation reduces environmental impact and supports a circular economy.

5.3. Lifecycle Management - Encourage lifecycle assessments and end-of-life recycling or repurposing

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

strategies

Encourage lifecycle assessments and implement strategies for end-of-life recycling or repurposing of access control systems. Evaluate the environmental impact at each stage from production to disposal to identify improvement opportunities. Design equipment for durability and easy disassembly to facilitate upgrades and recycling. Establish take-back programs or partner with certified e-waste recyclers to ensure responsible disposal. By managing the entire lifecycle effectively, the organisation minimises waste and promotes sustainable practices while maintaining system efficiency.

6. Social Responsibility

Ensure the solutions align with social sustainability goals.

6.1. User Privacy and Data Security

Protect user data by implementing robust security measures in access control systems to prevent unauthorised access and breaches. Ensure ethical data management practices by collecting only necessary information, obtaining explicit user consent, and complying with data protection regulations like GDPR. Encrypt sensitive data both in transit and at rest, and regularly update security protocols to address emerging threats. Train staff on data privacy principles and the importance of confidentiality. By prioritising user privacy and data security, the organisation upholds social responsibility and maintains trust with users.

6.2. Accessibility

Design access control systems that are inclusive and accessible to all users, including those with disabilities. Incorporate features like tactile feedback, audio cues, and adjustable interfaces to accommodate diverse needs. By prioritising accessibility, the Organisation upholds social responsibility and provides equal access to security systems for everyone.

6.3. Employee and Community Impact

Consider the social impact of production processes by ensuring fair working conditions throughout the supply chain. Select suppliers who adhere to ethical work practices, provide safe working environments, and respect workers' rights. Promote transparency by monitoring and auditing supplier practices. Support local communities through responsible sourcing and engagement in social initiatives. By addressing employee and community impact, the Organisation upholds social responsibility and contributes to positive societal outcomes.

6.3.1. The Equalities Act 2010

The Equality Act 2010 primarily addresses discrimination and promotes equality, but it indirectly impacts environmental and sustainability efforts. Through its focus on inclusivity, the Act encourages accessible green spaces, equitable urban planning, and diverse representation in environmental decision-making.
The Public Sector Equality Duty (PSED) requires public bodies to consider how their policies affect individuals with protected characteristics, influencing sustainable transport systems, energy policies, and urban designs. Businesses integrating the Act's principles into ESG strategies often align social equity with environmental goals, such as fair labour practices in green supply chains. The Act also underpins climate justice by protecting marginalized communities disproportionately affected by environmental issues. While not explicitly addressing sustainability, its framework fosters fairness and inclusion, which are essential to tackling ecological challenges equitably.

7. Governance and Compliance - Align with relevant regulations and industry standards.

Ensure that all access control systems adhere to relevant data protection laws such as the Data Protection Act 2018 (DPA 2018), UK GDPR, and other applicable regulations. Implement policies and procedures to protect personal and sensitive data, including secure data handling, storage, and processing practices. Regularly audit and update systems to maintain compliance with current laws. Provide staff training on legal obligations and data protection best practices. By strictly adhering to these regulations, the Organisation upholds governance standards and minimises legal and reputational risks.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

7.1. Ethical Considerations

Ensure the ethical use of technology, especially AI in biometric systems. Implement measures to prevent bias and discrimination by using diverse and representative datasets for AI training. Obtain informed consent from users before collecting biometric data, ensuring transparency about data usage and storage. Regularly audit AI systems for fairness, accuracy, and compliance with ethical standards. By addressing these ethical considerations, the organisation upholds governance standards and maintains user trust).

7.1.1. Facial recognition technology - Ethical use and deployment in video surveillance-based systems - Code of practice - environment and sustainability

BS 9347:2024 provides ethical guidance for using Facial Recognition Technology in access control systems, ensuring its deployment aligns with Environmental, Social, and Governance (ESG) principles.

- **Environmental**: Encourages the adoption of energy-efficient technology within access control systems to minimise environmental impact, support sustainability, and reduce energy consumption.
- **Social**: Emphasizes the importance of protecting individual privacy, ensuring that systems do not discriminate, and fostering trust by prioritising fairness and ethical handling of personal data in access-controlled environments.
- **Governance** highlights the need for transparent processes, accountability, and adherence to legal and ethical standards. It ensures organizations implement access control systems with transparent governance and secure management of sensitive data.

This standard ensures that facial recognition technology in access control systems is deployed responsibly, balancing innovation with ethical, environmental, and sustainable considerations.

7.2. Transparent Reporting

Commit to regular, transparent sustainability reporting. Openly share information about the organisation's environmental and social performance related to access control systems. Publish reports detailing progress on sustainability objectives, compliance with regulations, and any challenges faced. Ensure reports are accessible to stakeholders and follow recognised standards like the Global Reporting Initiative (GRI). By providing transparent reporting, the organisation demonstrates accountability and builds trust with stakeholders.

The **Global Reporting Initiative (GRI)** is an international independent organisation that provides a standardised framework for organisations to report on their environmental, social, and governance (ESG) performance. Established in 1997, GRI helps businesses, governments, and other entities understand and communicate their impacts on critical sustainability issues such as climate change, human rights, and corruption.

By following GRI's standards, organisations can produce transparent and comparable sustainability reports. This enables stakeholders including investors, customers, and the public to assess an organisation's commitment to sustainable practices and make informed decisions. The GRI standards are widely recognised and used globally, promoting accountability, and driving positive change toward sustainable development.

8. Strategic Goals and Targets

8.1. Strategic Goals

Establishing strategic environmental and sustainability goals involves setting targets across short-term, medium-term, and long-term horizons. Short-term goals focus on reducing waste by a specific percentage within a defined timeframe and enhancing energy efficiency throughout operations. Medium-term goals aim to decrease carbon emissions over the next decade by increasing the adoption of renewable energy sources. Long-term goals strive to achieve net-zero emissions and fully integrate circular economy principles, which involve keeping resources in use for as long as possible, extracting maximum value from them, minimizing waste, and promoting resource efficiency. Continuous evaluation is essential to monitor progress toward these milestones and ensure alignment with global sustainability standards.

The information below is for guidance purposes only on how you would achieve net-zero emissions over several years.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

- **Short-term Goals (1-2 years example and could be variable dependent on circumstances) -** Set specific, measurable goals, such as reducing energy consumption by a certain percentage.

  Set specific, measurable objectives like reducing energy consumption of access control systems by implementing energy-efficient hardware and software optimisations. Begin transitioning to sustainable materials in new devices. Establish baseline measurements for current environmental impact. Engage suppliers to enhance sustainability in the supply chain. Provide staff training on sustainable practices related to access control systems.

- **Medium-term Goals (3-5 years example and could be variable dependent on circumstances) -** Include goals like transitioning to recyclable materials for devices.

  Transition to using for example recyclable materials for all access control devices. Achieve a total energy consumption reduction from the set original baseline. Implement comprehensive recycling or take-back programs for obsolete equipment. Integrate renewable energy sources, such as solar power, into the access control infrastructure where feasible. Strengthen partnerships with suppliers who meet higher environmental standards. Enhance user engagement in sustainability initiatives.

- **Long-term Goals (5+ years example and could be variable dependent on circumstances) -** Aim for more ambitious targets, like achieving net-zero emissions across the access control system lifecycle.

  Aim to achieve net-zero emissions across the entire lifecycle of access control systems. This includes production, operation, and disposal phases. Invest in carbon offset projects to balance any remaining emissions. Foster innovation in sustainable technologies within the industry. Lead by example and share best practices with other organisations. Regularly review and update sustainability goals to align with new advancements and regulations.

The above is an example and not definitive. It is used for guidance purposes only and is dependent on your circumstances of how reasonably you can effectively reach the timeline milestones for net-zero emissions, as you can adjust the three milestone definitions years listed above to your desired length. Ultimately, achieving this is dependent on your circumstances.

8.2. Implementation Plan

The implementation plan for environment and sustainability focuses on integrating green practices across all operations, beginning with an energy audit and waste reduction measures. It includes training employees on sustainable practices, transitioning to renewable energy, and enhancing supply chain sustainability. Regular monitoring and reporting will ensure targets are met while fostering partnerships for innovation in eco-friendly technologies. Continuous improvement and stakeholder engagement are key to long-term success.

Actions and Initiatives - Detail the actions to be taken to achieve the sustainability goals.

Detail specific steps to achieve sustainability goals, such as upgrading to energy-efficient hardware, implementing recycling programs for outdated devices, and optimising software for lower energy consumption. Establish clear timelines and assign responsibilities to relevant teams. Launch initiatives to reduce carbon footprint, like integrating renewable energy sources into access control systems. Promote the adoption of sustainable materials in new equipment. Regularly monitor progress and adjust strategies as needed. Engage employees by encouraging suggestions for further sustainability improvements.

R&D Investments - Invest in research and development of sustainable technologies.

Invest in research and development of sustainable technologies for access control systems. Allocate funds to explore innovations like low-power biometric devices, eco-friendly materials, and energy-harvesting technologies. Collaboration with research institutions and industry experts to stay at the forefront of sustainability advancements. Encourage internal teams to experiment with prototype solutions that reduce environmental impact. Evaluate the feasibility and scalability of new technologies before full-scale implementation. Prioritise R&D projects that align closely with sustainability objectives.

Manufacturers should visit the UK government website to see if there is any R&D tax relief available for their products and services.

Partnerships - Collaboration with sustainable suppliers and industry bodies.

Collaboration with suppliers who prioritise sustainability and ethical practices. Establish partnerships with industry bodies and environmental organisations to share best practices and stay informed about new regulations. Negotiate contracts that include sustainability clauses and performance metrics. Participate in industry forums focused on sustainable development. Work together with partners to develop joint initiatives aimed at reducing the overall

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

environmental impact of the supply chain. Foster long-term relationships that support continuous improvement in sustainability efforts.

Employee Training - Implement training programs on sustainable practices for staff.

Implement training programs on sustainable practices for all staff involved with access control systems. Develop educational materials covering topics like energy efficiency, responsible sourcing, and waste reduction. Schedule regular workshops and provide online resources for continuous learning. Encourage employees to adopt sustainable practices in their daily tasks. Include sustainability objectives in performance evaluations to reinforce their importance. Recognise and reward staff contributions to sustainability goals to motivate ongoing engagement.

Resource Allocation - Outline the budget and resources allocated for sustainability initiatives.

Outline the budget and resources allocated for sustainability initiatives within the access control systems. Allocate funding for upgrades to energy-efficient equipment, R&D projects, training programs, and partnership activities. Ensure that financial planning includes long-term savings from reduced energy consumption and waste. Assign dedicated personnel or teams to manage sustainability projects. Monitor expenditures to ensure efficient use of resources. Adjust allocations as needed based on progress and changing priorities.

Stakeholder Engagement - Plan for engaging stakeholders, including customers, employees, suppliers, and the community.

Plan to engage stakeholders in sustainability efforts, including customers, employees, suppliers, and the community. Communicate goals and progress through reports, meetings, and social media. Solicit feedback and encourage active participation in initiatives. Organise events or campaigns to raise awareness about sustainability practices. Collaboration with community organisations on environmental projects. Use stakeholder input to refine strategies and improve the effectiveness of sustainability programs. Build strong relationships to foster a shared commitment to environmental responsibility.

9. Monitoring and Evaluation

After you have implemented your strategic plan targets and goals, you will need to make sure its momentum is maintained by defining your Key Performance Indicators (KPIs) that are reported to maintain continuous improvement.

- **Performance Indicators (KPIs) -** Define KPIs to measure progress against sustainability goals.
- **Reporting Mechanisms -** Establish regular reporting mechanisms to communicate progress internally and externally.
- **Continuous Improvement -** Incorporate a feedback loop for continuous improvement of the sustainability practices.

Define KPIs specific to access control systems to measure progress against sustainability goals.

Examples include:

- Energy Consumption Reduction - Percentage decrease in energy usage by access control devices annually.
- Use of Sustainable Materials - Proportion of access control equipment made from recyclable or non-toxic materials.
- E-Waste Management - Amount of decommissioned access control hardware that is recycled or repurposed.
- Carbon Emissions - Reduction in greenhouse gas emissions associated with the operation of access control systems.
- Compliance Rate - Percentage of access control components meeting environmental regulations and standards.

Regular monitoring of these KPIs helps assess performance and identify areas for improvement.

9.1. Reporting Mechanisms

Establish regular reporting mechanisms focused on the sustainability of access control systems. Generate quarterly or annual sustainability reports detailing progress on KPIs, achievements, and challenges. Share these reports internally with management and staff, and externally with stakeholders like customers and partners. Utilise dashboards or scorecards to present data in an accessible format. Ensure that reporting aligns with recognised standards such as the Global Reporting Initiative (GRI). Transparent reporting fosters accountability and keeps sustainability goals at the forefront of access control management.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

9.2. Continuous Improvement

Incorporate a feedback loop for continuous improvement of sustainability practices in access control systems. Regularly review KPI data and gather feedback from users, technicians, and other stakeholders involved with access control. Identify inefficiencies or new opportunities for enhancing sustainability, such as adopting advanced energy-saving technologies or improving recycling programs. Update strategies and action plans based on findings and technological advancements. Encourage the access control team to suggest innovations and stay informed about industry best practices. By embracing continuous improvement, the Organisation ensures ongoing progress toward sustainability objectives within access control operations.

10. Risk Management

Risk management can identify and mitigate risks to achieve sustainability efforts, such as regulatory changes or supply chain disruptions. Mitigation strategies to reduce these risks, ensuring the framework remains resilient and adaptable.

10.1. Identify Risks

Identify potential risks to sustainability efforts in access control systems, such as:

- **Regulatory Changes -** New environmental or data protection laws may require significant adjustments to existing systems or practices.
- **Supply Chain Disruptions -** Shortages of sustainable materials or components could hinder the deployment of eco-friendly access control devices.
- **Technological Obsolescence -** Rapid advancements may render current systems outdated, leading to increased waste and resource expenditure.
- **Cybersecurity Threats -** Security breaches can compromise both system integrity and user data, undermining trust, and compliance efforts.
- **Financial Constraints -** Budget limitations might restrict investments in sustainable technologies or necessary upgrades.

10.2. Mitigation Strategies

Develop strategies to mitigate these risks, and ensuring the framework remains resilient and adaptable:

- **Regulatory Monitoring -** Stay informed about legislative changes to proactively adjust compliance strategies for access control systems.
- **Supplier Diversification** - Partner with multiple sustainable suppliers to reduce dependency and mitigate supply chain disruptions.
- **Modular System Design -** Implement flexible, upgradeable access control solutions to accommodate technological advancements without full replacements.
- **Enhanced Cybersecurity Measures -** Invest in robust security protocols to protect systems and data, maintaining user trust and compliance.
- **Financial Planning -** Allocate dedicated budgets for sustainability initiatives and explore external funding or incentives to support investments.

11. Technology Cross Collaboration and the User-centric Approach

Ensure the framework for access control systems is flexible to adapt to evolving technologies. Design systems with modular architectures that allow for easy upgrades and integration of new features, such as advanced biometrics or AI-driven analytics. Stay informed about emerging trends and standards in access control to incorporate innovations that enhance sustainability and security. Implement scalable solutions that accommodate growth and technological shifts without requiring complete system overhauls. This adaptability minimises waste and ensures the long-term viability of access control infrastructure.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

Implementation of a framework to achieve a cross-functional collaboration by involving various departments such as IT, HR, Facilities Management, and Compliance in developing and implementing the sustainability framework for access control systems. This collaboration ensures that all perspectives are considered, from technical feasibility to regulatory compliance and user experience. Joint efforts facilitate aligning sustainability goals with organisational objectives and operational needs. Regular interdepartmental meetings and workshops can foster shared understanding and commitment. Collaboration planning enhances the effectiveness and adoption of sustainable practices in access control solutions.

Ensuring that sustainable solutions in access control systems do not compromise usability or security requires a user-centric approach that prioritises the end-user experience. Organisations can implement environmentally friendly practices without sacrificing functionality or safety by focusing on users' needs and preferences. This balance is essential for the successful adoption of sustainable technologies in access control. Design intuitive solutions that do not compromise usability or security in the pursuit of sustainability. Gather user feedback to understand stakeholder needs and preferences, ensuring sustainable measures enhance rather than hinder system interaction. For example, energy-saving features that do not slow down authentication processes should be implemented. Balancing sustainability with user convenience and security maintains system effectiveness and promotes user acceptance of sustainable initiatives.

By following this structure, you can create a comprehensive sustainability framework that guides your organisation towards more responsible and sustainable practices in access control solutions.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

This document was created by the Access and Asset Protection Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

The British Security Industry Association's Access and Asset Protection Section brings together companies involved in areas of security providing physical products to stop unwanted people from accessing property or valuables and the electronic measures that can, optionally, control them.

The section includes member companies involved in the manufacture, supply and installation of solutions that restrict, control, and monitor the movement of people, assets, or vehicles in, out and around a building or site. This includes physical protection methods, such as security doors, fencing, locks, barriers, safes, and strong rooms, rising screens, etc and the electronic access control systems that control them, allow authorised persons in, and keep undesired people out.

Access control products are subject to fast-moving technological development. The section aims to raise awareness amongst end-users and specifiers of the different types of equipment that are available, the applicable standards and the most appropriate environments for using them.

The Access and Asset Protection Section sits in a strong position when it comes to lobbying for consistent standards and regulations. Access control products are subject to fast-moving technological development. A major focus of the section is to raise awareness amongst end-users and specifiers of the different types of equipment that are available and the most appropriate environments for using them.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards, and legislative bodies. For more information contact the BSIA.

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.