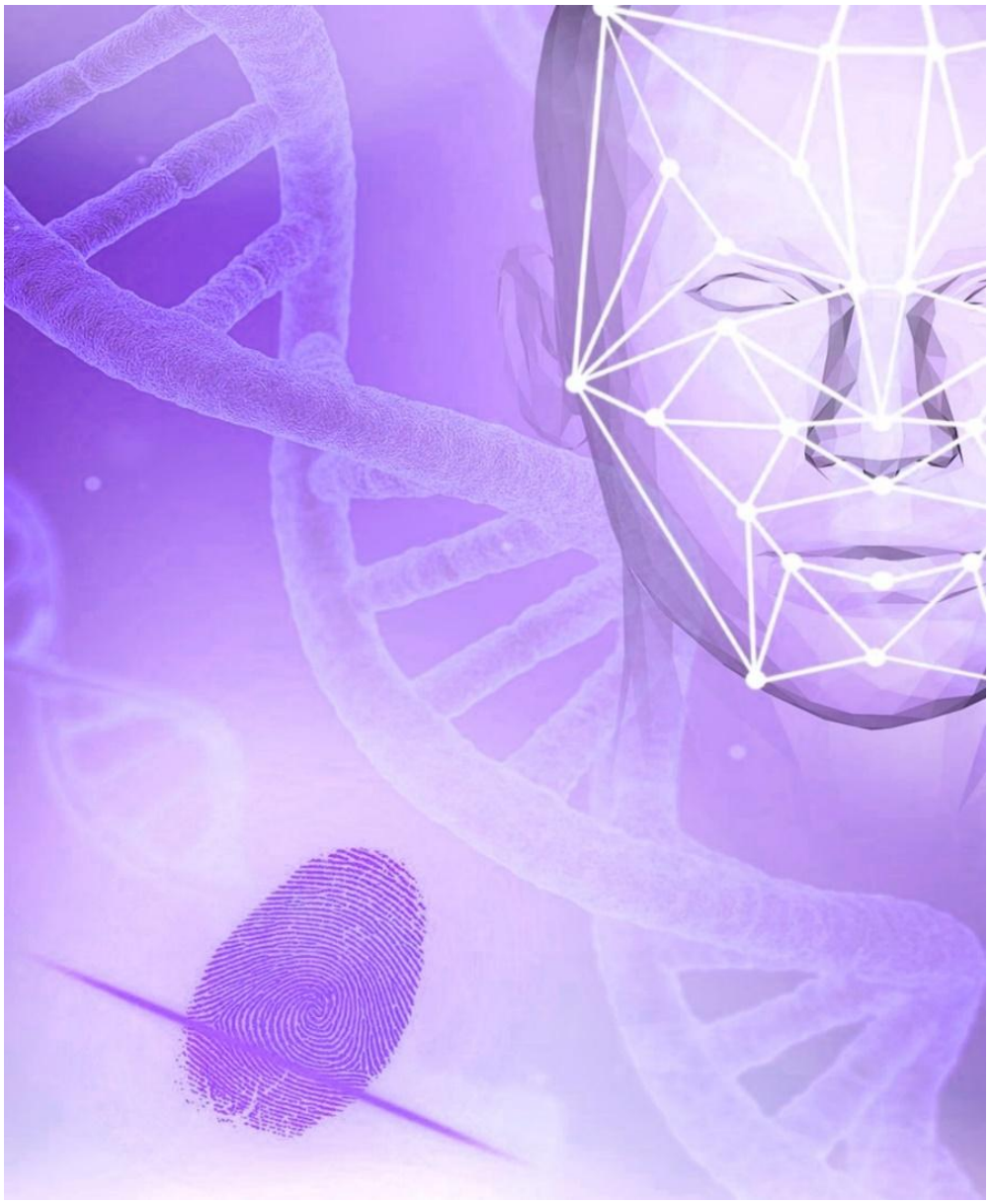
SCOTTISH BIOMETRICS COMMISSIONER

RISK MANAGEMENT POLICY &
STRATEGIC RISK REGISTER



Safeguarding our biometric future

Document Control:

Title	Risk Management Policy & Strategic Risk Register
Prepared by	Director
Reviewed by	SBC Team
Date	November 2025

Introduction

This document sets out the Scottish Biometric Commissioner's (SBC) risk management plan in line with the Strategic Plan, annual business plan for the period and the Business Continuity Policy. It sets out our appetite for risk and how we assess the risks to achieving our strategic outcomes. It should be read in conjunction with our Risk Management Policy, within the Scheme of Governance and Risk Handbook published on our website.

Risk Appetite

Our current overall risk appetite is defined as **OPEN.** This means the SBC will continue to encourage new thinking and invest in people, systems and processes that will enable the organisation to achieve continuous improvement in the quality and user-focus of our services.

The SBC aims to balance the methods it uses to control risks so it can both support innovation and the imaginative use of resources and continue to provide best value. The SBC will seek to control all probable risks which have the potential to:

- cause significant harm to users, staff, and stakeholders
- compromise severely the reputation of the organisation
- have financial consequences that could endanger the organisation's viability
- jeopardise significantly the organisation's ability to carry out its core functions
- threaten the organisation's compliance with law and regulation

Descriptors

AVERSE	Avoidance of any risk exposure recognising this will have little or no potential for reward/return
MINIMAL	Willing to accept some low risks, while maintaining an overall preference for safe delivery options despite the probability of these having mostly restricted potential for reward/return
CAUTIOUS	Tending towards exposure to modest levels of risk to achieve acceptable, but possibly unambitious outcomes
OPEN	Prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk
HUNGRY	Eager to be innovative and accept the associated high-risk levels to secure successful outcomes and meaningful reward/return

Risk Appetite

	Appetite	Risk
1	**OPEN**	The SBC fails to deliver the Strategic Plan and fulfil statutory duties due to insufficient funding, resources or the inability to influence external factors and/or the environment within which we operate
2	**OPEN**	The SBC fails to provide value, demonstrate outcomes and the positive impact of our work and does not engage effectively and timely with stakeholders or specific-interest groups within and across the policing and community justice landscape or fails to recognise opportunities to build and manage effective stakeholder relationships
3	**HUNGRY**	The SBC fails to ensure corporate governance arrangements, policies and procedures, scrutiny are accountable, appropriate and effective, and are linked to output and performance
4	**CAUTIOUS**	The SBC fails to maintain business continuity and does not have effective cyber resilience plans

5	**CAUTIOUS**	The SBC fails to recruit and retain the right professionals who are supported and developed appropriately to ensure the organisation has a skilled and motivated workforce
6	**OPEN**	The SBC fails to timeously or effectively adapt to threats and opportunities brought by technological, economic, political, environmental, legal and structural public sector change

Overview

Strategic Risks are set and aligned with the Strategic Plan and all four of our strategic objectives and run for the 4-years of the Plan. They are reviewed quarterly through Strategic Management Team Meetings. The strategic risk register is the mechanism by which the links are made between strategic aims and operational delivery and performance of services.

Review

As part of internal control and effective business planning the SBC will review the key risks associated with achievement of the SBC's strategic objectives. This will involve assessing the impact of all potential key risks (not only financial risks) and considering how they should be managed. The three main objectives of the quarterly review of the risk register will be to:

- assess existing controls (the measures in place to reduce or limit risk)
- determine the appropriate response to each risk
- agree future review procedures

The strategic risk register will be discussed with the Advisory Audit Board.

SBC staff will discuss and rate the inherent likelihood of each risk occurring, and its impact on quality, cost and timescales should it occur. This is done by assessing and awarding a numerical value between 1 and 5 as to the likelihood of the risk occurring and to the level of impact. These values are then multiplied, and an overall score is awarded.

Controls and mitigating factors are discussed and the risk is re-assessed. Any further planned controls to mitigate the risk are recorded, and a plan action identified.

Risk Scoring Matrix

Table 1 – Impact Scores

Domains	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
	Negligible	Minor	Moderate	Major	Significant
Statutory duty/governance	No or minimal impact or breach of statutory duty	Breach of statutory legislation	Single breach in statutory duty. Challenging external recommendations	Enforcement action. Multiple breaches in statutory duty. Qualified audit	Multiple breaches in statutory duty. Prosecution. Severely critical report
Adverse public reaction	Rumours. Potential for public concern	Local media coverage – short term reduction in public confidence	Local media coverage – long term reduction in public confidence	National media coverage with service well below public expectation	National media coverage with service well below public expectation. Scottish Parliament concerned. Total loss of public confidence
Business objectives	Insignificant cost increase	<5% over budget	5-10% over budget	Non-compliance with 10% over budget. Key objectives not met	Incident leading >25% over budget. Key objectives not met
Business impact	Loss/interruption >1 week	Loss/interruption >2 weeks	Loss/interruption >1 month	Loss/interruption >2 months	Permanent loss of service
Breach of confidentiality/data loss	No significant reflection on any individual. Media interest unlikely. Minor breach	Damage to individual's reputation. Possible media interest. Potential serious breach e.g. files were encrypted	Damage to team's reputation. Some local media interest that may not go public. Serious potential breach and risk assessed high e.g. unencrypted file lost	Damage to service/organisation's reputation. Local media coverage. Serious breach of confidentiality	Damage to SBC reputation. National media coverage. Serious breach with potential for further consequences to individuals

Table 2 – Likelihood Scores

Likelihood	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency	This will probably never happen / recur	Do not expect it to happen / recur but it is possible	Might happen or recur occasionally	Will probably happen / recur but is not a persistent issue	Will undoubtedly happen / recur, possibly frequently

Table 3 – Risk Rating (Impact x Likelihood)

Impact Scores	Likelihood Scores				
	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost Certain
1 Negligible	1	2	3	4	5
2 Minor	2	4	6	8	10
3 Moderate	3	6	9	12	15
4 Major	4	8	12	16	20
5 Significant	5	10	15	20	25

For grading risk, the scores obtained from the risk matrix are assigned as follows:

Score	Grade
1-5	VERY LOW risk
6-10	LOW risk
12-15	MODERATE risk
16-20	HIGH risk
25	VERY HIGH risk

Risk appetites can be aligned to the above matrix as follows:

Risk Grade	Risk Appetite
VERY LOW risk	HUNGRY
LOW risk	OPEN
MODERATE risk	CAUTIOUS
HIGH risk	MINIMAL
VERY HIGH risk	AVERSE

ID	Risk Description	Gross Risk			Mitigation/Control Action	Residual Risk			Risk Appetite
		Likelihood	Impact	Score		Likelihood	Impact	Score	
SR 1	The SBC fails to deliver the Strategic Plan and fulfil statutory duties due to insufficient funding, resources or the inability to influence external factors and/or the environment within which we operate **Cause:** ▪ Inability to influence Scottish Parliament as sole funding source ▪ Single year funding arrangements to support a four-year Strategic Plan ▪ As most UK policing biometric databases are funded by the Home Office it is possible, policy decisions taken by UK Government may conflict with the views of the Scottish Parliament **Consequence:** ▪ Negative impact on our ability to deliver on strategic outcomes ▪ Reputational damage ▪ Inability to proactively consider additional operational work ▪ Inability to grow capacity and to the standard needed to maintain motivated and skilled staff	3	5	15 (Moderate Risk)	Fully engaged in budget process including with SPCB through budgetary cycle and access to contingency funding (where necessary) Careful consideration of resource requirements through business planning process informed by risk Strategic Plan laid before Parliament with resourcing scenarios and indicative budgeting Medium-term Financial Strategy published which includes worst case scenarios Sound governance arrangements and budgetary management Agreement to second in additional resource for two-years – this resource is aligned to the operational needs of the Strategic Plan	2	5	10 (Low Risk)	**OPEN**

SR 2	The SBC fails to provide value, demonstrate outcomes and the positive impact of our work on the Scottish public; does not engage effectively and timely with stakeholders or specific-interest groups within and across the policing and community justice landscape; fails to recognise opportunities to build and manage effective stakeholder relationships **Cause:** ▪ Communications are unclear and/or not directed to the correct audience ▪ Insufficient management of key relationships ▪ Lack of interest or timely engagement with specific-interest groups **Consequence:** ▪ Low levels of public and stakeholder support ▪ Lack of trust and confidence in our ability ▪ Stakeholder voice not heard ▪ Groups feel disenfranchised ▪ Incomplete or misinformation disseminated ▪ Loss of credibility	3	5	15 (Moderate Risk)	Established mechanisms to support proactive public and stakeholder engagement SBC represented on all relevant UK and Scottish strategic stakeholder forums concerned with the management of biometric databases and technologies within statutory remit Statutory Advisory Group established a strong framework for stakeholder engagement and support SBC jointly produces and publishes reports with key stakeholders which strengthens partnership working and ensures best value for the public purse Communications & Engagement Strategy published Media Management Policy published Respond to consultations and proactively publish articles on new and emerging biometric technologies Provide evidence and lay all statutory reports before Parliament **Forthcoming actions:**	2	3	6 (Low Risk)	**OPEN**

					Communications & Engagement action plan to be developed which considers how best to engage with wider audience				
SR 3	The SBC fails to ensure corporate governance arrangements, policies, procedures, scrutiny are all accountable, appropriate and effective, and are linked to output and performance **Cause:** ▪ Corporate governance arrangements are not effectively discharged ▪ Unclear policies and procedures ▪ Shared services fail to deliver e.g. resources not aligned ▪ Insufficient performance management **Consequence:** ▪ Loss of credibility ▪ Data breach/loss ▪ Information and records management does not comply with legislative requirements ▪ Decreased public confidence ▪ Qualified audit ▪ Failure to deliver strategic objectives ▪ Shared services do not meet SBC requirements	2	5	10 (Low Risk)	Strong governance structures in place through the scheme of delegation and control, internal and external audit plans, handbooks and policies covering all corporate functions Strong relationship with the Scottish Parliamentary Corporate Body and Advisory Audit Board Shared services agreement in place Regular review of corporate policies which are presented to Advisory Audit Board Ongoing performance, governance and outcomes oversight	2	2	4 (Very Low Risk)	**HUNGRY**
SR 4	The SBC fails to maintain business continuity and does not have effective cyber resilience plans **Cause:** ▪ Untested business continuity	3	5	15 (Moderate Risk)	Business Continuity Plan and policy reviewed regularly with appropriate testing and liaison with third parties	3	4	12 (Moderate Risk)	**CAUTIOUS**

	▪ Lack of cognisance towards increased cyber security threats ▪ Lack of staff training ▪ Staff not cross-functional ▪ Successful cyber attack ▪ Lack of staff due to absence or turnover **Consequence:** ▪ Mismanagement of incident ▪ Loss of information and data ▪ Prolonged loss of access to systems ▪ Inability to function effectively and deliver on strategic outcomes ▪ Reputational damage ▪ Major data breach ▪ Financial fraud ▪ Action by external stakeholder – ICO, Audit Scotland				Monitoring of external sources of information, acting as needed ICT policies in place SBC operate hybrid working Mandatory ICT and cyber security training for all staff Stringent internal controls introduced re financial processing between the SBC and SPSO				
SR 5	The SBC fails to recruit, retain and effectively manage the right professionals who are supported and developed appropriately to ensure the organisation has a skilled and motivated workforce **Cause:** ▪ Prolonged staff absence ▪ Staff failing to meet the requirements of their job description ▪ HR element of shared services agreement fails to meet requirements ▪ HR policies not fit for purpose **Consequence:** ▪ Staff turnover ▪ Inability to deliver strategic outcomes ▪ Reputational damage	4	4	16 (High Risk)	Independent annual staff engagement and wellbeing survey commissioned through an external HR professional Informal and formal staff meetings provide opportunities for staff training and development as well as a framework for performance management Range of policies available which are reviewed regularly Personal Development Plans occur annually along with regular 121 meetings which focus on performance	3	4	12 (Moderate Risk)	**CAUTIOUS**

	▪ Low staff morale				Organisational restructure of Director post who also acts as the Corporate Services Manager – allows for added support to Commissioner and further operational resource and resilience Two-year secondment of subject matter expert into the SBC strengthens stakeholder relationships, offers new learning and knowledge exchange within the workforce while offering resilience and operational experience **Forthcoming actions:** Amendments to HR policies to reflect working practices within a small organisation In-depth review of shared services agreement to ensure all aspects remain fit for purpose and meet the needs of the organisation				
SR 6	The SBC fails to timeously or effectively adapt to threats and opportunities brought by technological, economic, political, environmental, legal and structural public sector change **Cause:** ▪ Lack of understanding or awareness ▪ Lack of staff training	3	3	9 (Low Risk)	Stakeholder engagement Horizon scanning The SBC represented on all relevant UK and Scottish strategic stakeholder forums concerned with the management of biometric databases and technologies within statutory remit	3	2	6 (Low Risk)	**OPEN**

	▪ Lack of resource to conduct effective horizon scanning **Consequence:** ▪ Inability to deliver strategic outcomes ▪ Reputational damage among key stakeholders				Strong working relationship with SPCB and Parliament/Ministers Close working relationship with role holder in NI, England & Wales Staff training identified through annual Personal Development Plans				