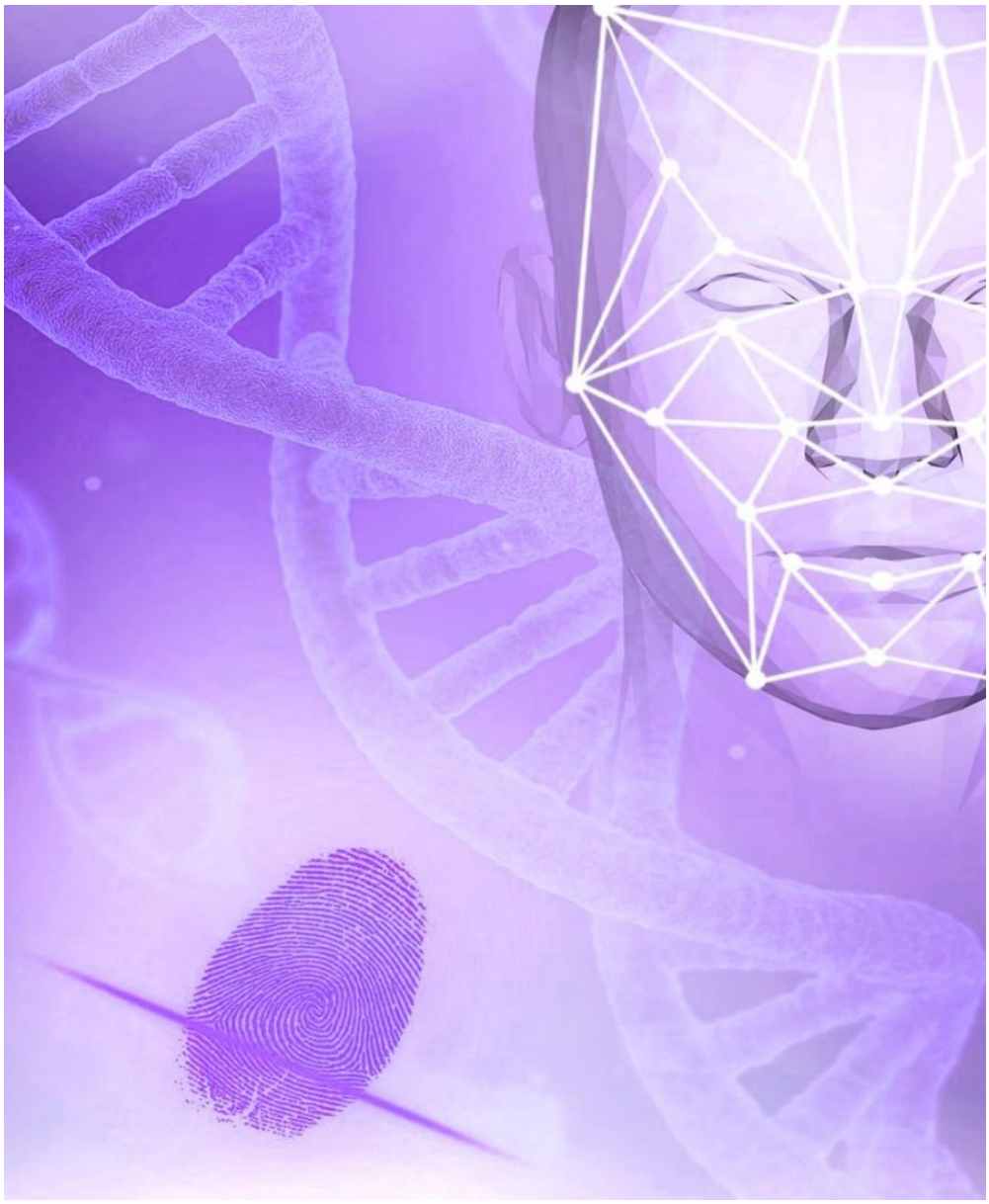
SCOTTISH BIOMETRICS COMMISSIONER

RISK MANAGEMENT POLICY &
STRATEGIC RISK REGISTER



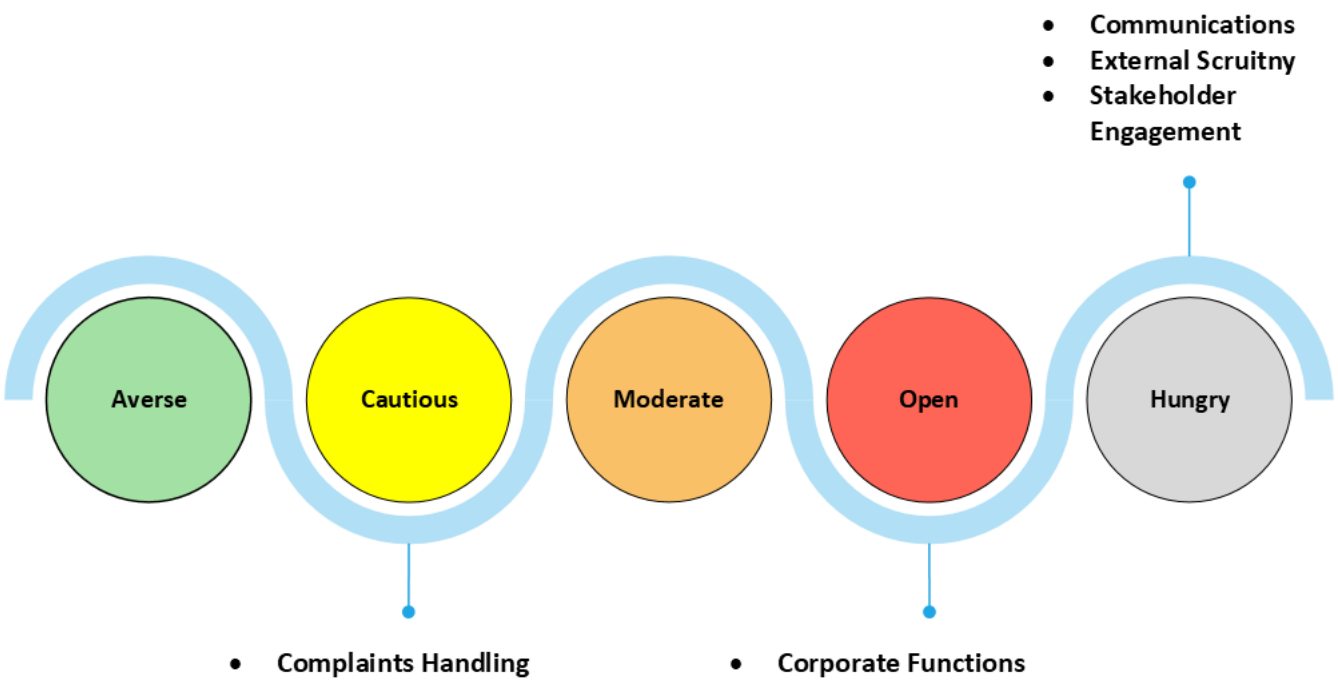
Safeguarding our biometric future

Introduction

This document sets out the Scottish Biometric Commissioner's (SBC) risk management plan in line with the strategic plan and annual business plan for the period. It sets out our appetite for risk and how we assess the risks to achieving our business plan. It should be read in conjunction with our Risk Management Policy, within the Governance and Risk Management 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 a best value public service. The SBC will seek to control all probable risks which have the potential to:

- cause significant harm to service users, staff, visitors and other 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

AVOID	No appetite. Not prepared to accept any risks
AVERSE	Prepared to accept only the very lowest levels of risk, with the preference being for ultra-safe delivery options, while recognising that these will have little or no potential for reward/return
CAUTIOUS	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
MODERATE	Tending always towards exposure to only modest levels of risk in order 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 seek original/creative/pioneering delivery options and to accept the associated substantial risk levels in order to secure successful outcomes and meaningful reward/return

Appetite for each function

Function	Appetite	Detailed statement
Corporate Functions	**OPEN**	We will accept modest levels of risk in pursuit of innovation, effectiveness and efficiency. However, not to the extent where there is any compromise to overall good governance or to the best practice arrangements as detailed in our scheme of delegation and control
Communications	**HUNGRY**	We will explore creative and innovative approaches to communications in pursuit of our general function to promote public awareness and understanding of how biometric data is used for policing and criminal justice purposes. When appropriate, we will accept substantial risk levels to exploit novel or innovative methods of communication
External Scrutiny	**HUNGRY**	We will design our external review activities in a way that minimises the burden of scrutiny on those to whom our functions extend in line with the Crerar Principles (2007) to regulation, audit and inspection. Our activities will be informed at all times by considerations of proportionality, necessity, and public focus. When possible, our approach will be based on validated self-assessment and in doing so we are prepared to accept substantial levels of risk
Complaints Handling	**CAUTIOUS**	We will accept only low levels of risk that could undermine our provision of systems and processes that enable us to achieve continuous improvement in the quality and user-focus of our services
Stakeholder Engagement	**HUNGRY**	We will seek and implement innovative and pioneering approaches to engage effectively and efficiently with our functional bodies, establishing strong relationships to ensure our work is understood

Overview

The Strategic Risks will be set at the start of each financial year, as part of the business planning process involving all staff. The strategic risk register is the mechanism by which the links are made between strategic aims and operational delivery and performance of services. Risks will be monitored regularly as per our Governance structure.

Through a risk session, SBC staff will compile an overall list of the key risks confronting the organisation and which threaten achievement of the SBC's strategic and business objectives.

Review

As part of their responsibility for internal control and as part of an effective business planning process SBC staff will meet at least quarterly to review the key business risks associated with achievement of the SBC's strategic objectives. At this time they will judge the impact of all potential key risks (not only financial risks) and consider how they should be managed. The five main objectives of the quarterly review of the risk register will be to:

- discuss, evaluate and agree the list of key business risks which might affect the ability to deliver objectives
- assess existing controls (the measures in place to reduce or limit risk)
- determine the appropriate response to each risk
- allocate responsibility for managing each risk
- and agree future review procedures.

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

Risk Evaluation and Response

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 as being either low, medium or high.

Controls and mitigating factors are then discussed and determined and the risk is re-assessed. Any further planned controls to mitigate the risk are recorded, and the business 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 hour	Loss / interruption >8 hours	Loss / interruption >1 day	Loss / interruption >1 week	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 score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Frequency (how often might it / does it happen)	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)

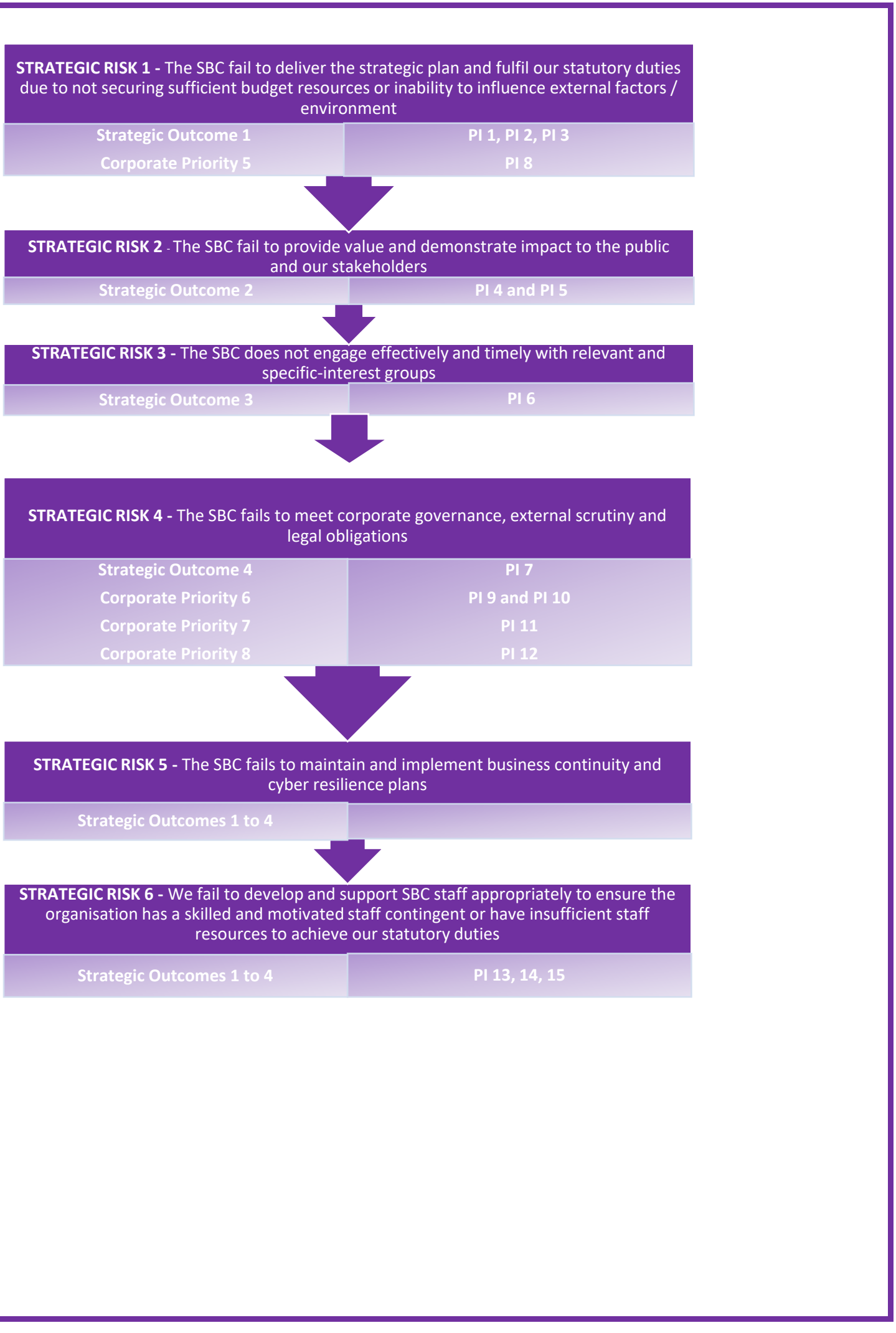
Impact Scores	**Likelihood Scores**				
	1	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
1 Negligible	1	2	3	4	5
2 Minor	2	4	6	8	10
3 Moderate	3	6	9	12	15
4 Major	4	8	12	16	20
5 Significant	5	10	15	20	25

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	MODERATE
HIGH risk	CAUTIOUS
VERY HIGH risk	AVERSE


STRATEGIC RISK 1 - The SBC fail to deliver the strategic plan and fulfil our statutory duties due to not securing sufficient budget resources or inability to influence external factors / environment
Strategic Outcome 1
Corporate Priority 5
PI 1, PI 2, PI 3
PI 8
STRATEGIC RISK 2 - The SBC fail to provide value and demonstrate impact to the public and our stakeholders
Strategic Outcome 2
PI 4 and PI 5
STRATEGIC RISK 3 - The SBC does not engage effectively and timely with relevant and specific-interest groups
Strategic Outcome 3
PI 6
STRATEGIC RISK 4 - The SBC fails to meet corporate governance, external scrutiny and legal obligations
Strategic Outcome 4
Corporate Priority 6
Corporate Priority 7
Corporate Priority 8
PI 7
PI 9 and PI 10
PI 11
PI 12
STRATEGIC RISK 5 - The SBC fails to maintain and implement business continuity and cyber resilience plans
Strategic Outcomes 1 to 4
STRATEGIC RISK 6 - We fail to develop and support SBC staff appropriately to ensure the organisation has a skilled and motivated staff contingent or have insufficient staff resources to achieve our statutory duties
Strategic Outcomes 1 to 4
PI 13, 14, 15

ID	Risk Appetite	Risk Description	Strategic Objective	Gross Risk			Mitigation / Control Action	Residual Risk		
				Likelihood	Impact	Score		Likelihood	Impact	Score
SR 1	Moderate	The SBC fail to deliver the strategic plan and fulfil our statutory duties due to not securing sufficient budget resources or inability to influence external factors / environment **Cause:** ▪ Inability to influence Scottish Parliament as sole funding source particularly in relation to the expansion of the remit functions of the SBC to include UK-wide policing bodies operating in Scotland ▪ Single year funding arrangements to support a four-year strategic plan ▪ As the majority of 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 grow capacity, where and to standard needed to maintain motivated and skilled staff	SO 1	5	5	25 (very high)	Fully engaged in budget bid process, careful consideration of resource requirements through business planning process, engagement with staff representatives The Commissioner sits on relevant UK strategic forums to monitor Home Office policy against the devolution consequences and Scottish interests The Commissioner has regular meetings with SG Police Division officials to discuss potential areas of conflicting interest Any decision on expansion of remit approved by Scottish Ministers under Section 2(7) of the SBC Act will require the Commissioner to conduct a business impact assessment. If the Commissioner's determination is that such expansion of remit requires additional resource, then the SPCB will need to provide the Commissioner with funding	5	3	15 (moderate)

							required before the additional responsibilities can be undertaken			
SR 2	Open	The SBC fail to provide value and demonstrate impact to the public and our stakeholders **Cause:** ▪ We do not communicate clearly and openly about our role and function ▪ Insufficient management of key relationships ▪ Limited ability / resource to engage effectively with target audience and promote the role of the SBC **Consequence:** ▪ Low levels of public and stakeholder support ▪ Lack of trust and confidence in our ability to deliver our statutory functions ▪ Stakeholder voice not heard	SO 2	3	5	15 (moderate)	Mechanisms have been established to support proactive stakeholder engagement and the Commissioner sits on all relevant UK and Scottish strategic stakeholder forums concerned with the management of biometric databases and technologies within our statutory remit. This, combined with the Commissioner's statutory advisory group establishes a strong framework for stakeholder engagement and support **Forthcoming actions:** Targeted work focussed on engagement and communications will be sourced (and resourced as appropriate) throughout the 2023/24 financial year to enhance our external visibility and awareness raising capabilities	2	3	6 (low)
SR 3	Open	The SBC does not engage effectively and timely with relevant and specific-interest groups **Cause:** ▪ Lack of interest or timely engagement ▪ Unclear expectations **Consequence:**	SO 3	3	4	12 (moderate)	Mechanisms have been established to include relevant groups within our stakeholder engagement plans. Regular horizon scanning to ensure we keep abreast of all groups (new and emerging)	3	3	9 (low)

		▪ Groups feel disenfranchised ▪ Loss of credibility ▪ Incomplete information								
SR 4	Hungry	The SBC fails to meet corporate governance, external scrutiny and legal obligations **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	SO 4	2	5	10 (low)	Strong governance structures in place through the scheme of control, internal and external audit plans. Strong relationship with the Scottish Parliamentary Corporate Body and through our Advisory Audit Board. Strong relationship and shared services agreement with SPSO which covers variety of functions (HR, Payroll, ICT, H&S) **Forthcoming actions:** Annual review of all corporate policies to be conducted systematically throughout the year and presented to Advisory Audit Board	1	2	2 (very low)
SR 5	Moderate	The SBC fails to maintain and implement business continuity and cyber resilience plans **Cause:** ▪ Untested business continuity plan ▪ Sole reliance on shared services agreement with SPSO ▪ Lack of cognisance towards increased cyber security threats	SO 1 - 4	4	5	20 (high)	Business Continuity Plan will be reviewed regularly with appropriate testing and liaison with third parties. Agreed approach in relation to disruption to business. Monitor external sources of information and act on plans as needed. Agreed shared services ICT policies in place	3	4	12 (moderate)

		▪ Lack of staff training ▪ Staff not working across-functions, lack of knowledge across roles ▪ 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 digital platforms / systems ▪ Inability to function effectively and deliver on strategic outcomes ▪ Reputational damage ▪ Major data breach ▪ Financial fraud ▪ Action by external stakeholder – ICO, SPSO, Audit Scotland					with annual mandatory ICT and cyber security training for staff Participation in Scottish Business Resilience Centre simulated cyber exercises continues as relevant SBC is now Cyber Essentials Accredited **Forthcoming actions:** Development of Cyber /Resilience Security Plan in partnership with SPSO through shared ICT service arrangements Further stringent internal controls to be introduced re financial processing between SBC and SPSO			
SR 6	Open	We fail to develop and support SBC staff appropriately to ensure the organisation has a skilled and motivated staff contingent or have insufficient staff resources to achieve our statutory duties **Cause:** ▪ The very nature of designing and standing up an entirely new public body whilst simultaneously recruiting its entire compliment of staff precluded both certainly in terms of future demand, and the possibility of pursuing the sorts of conventional modes of	SO 1 - 4	4	4	16 (high)	Strong and effective recruitment policies and mechanisms available through shared services agreement. Developed in-house policies including Working for the SBC Handbook; Personal Development Discussions occur annually **Forthcoming actions:** Implementation of Learning & Development plan Commissioner to have discussion with SPCB in June re their role and	3	3	9 (low)

		training and induction that would have been possible within an already established organisation ▪ Combination of ever increasing demand for external engagement and a single operational resource means the Commissioner is regularly required to participate in hands-on operational activity. This is not in keeping with the status or role requirement of the Commissioner ▪ Limited cross-over functions knowledge and awareness **Consequence:** ▪ Staff turnover ▪ Inability to deliver strategic outcomes ▪ Reputational damage ▪ Role of Commissioner must regularly exceed contracted hours to meet increasing demands on their time resulting in a residual sustainability risk					to submit a growth bid for an additional member of staff in September (in line with original policy memoranda that accompanied the SBC Bill) so that additional resource can be recruited and be in place by the start of 2024/25 to mitigate the sustainability risk			