

## Appendix B – Overview of Joint Strategic Risk Register

1	Failure to deliver against objectives set out in the Police and Crime Plan.
2	Inability to deliver continuity of service.
3	Critical incident or other external incident that has a sustained and significant demand on policing resources.
4	An ineffective Criminal Justice System with the region.
5	Reduction in partnership services due to financial constraints and a lack of integrated planning.
6	Failure to deliver the National Emergency Services Network (ESN) to Northumbria Police on time and to budget.
7	Insufficient resources, in terms of capacity and capability (skills), to meet current or future policing demands.
8	Insufficient resources, in terms of capacity and capability (health and wellbeing), to meet current or future policing demands.
9	Litigation, legal action and/or prosecution of the Force and/ or individuals by former officers or staff members.
10	Death in custody/death or serious injury following police contact.
11	Other adverse or critical incident, as a result of police action or omission.
12	Corrupt behaviour by an officer or police staff member.
13	Ineffective response to complaints or service recovery.
14	Failure to achieve ISO/IEC 17025 accreditation for digital device examination and impact on digital forensic examinations.
15	Force/ OPCC or an associated individual acts in a discriminatory way.
16	Failure to comply with the requirements of the General Data Protection Regulation.
17	Further cuts to Home Office Police Grant Funding.
18	Failure to manage annual budget.
19	Reduced effectiveness of Treasury Management.
20	Financial Risks arising as a result of exit from European Union.

21	Failure to dispose of the former HQ site as valued within the MTFS.
22	Ineffective delivery of the Force Estates Strategy.
23	Major disruption to use of key buildings, facilities or other assets and resources.
24	Estate risks around electrical and gas safety, water hygiene, asbestos containing materials and fire safety.
25	The loss or inappropriate disclosure of sensitive data or information.
26	Ageing IT infrastructure and implementation of future strategy.
27	A malicious intent to compromise information systems or access information or data.
28	Inability to maximise the opportunities from collaboration.
29	Data quality affecting business and operational decision making and compliance with national standards.

Summary of changes since last report

<b>Likelihood</b>	<b>VERY HIGH (5)</b>	6			
	<b>HIGH (4)</b>				
	<b>MEDIUM (3)</b>		11 14 20 26	16	
	<b>LOW (2)</b>		3 4 5 23 29	1 7 8 9 10 12 21 24 25 27 28	15 17
	<b>VERY LOW (1)</b>	2	19 22	13 18	
	<b>VERY LOW (1)</b>	<b>LOW (2)</b>	<b>MEDIUM (3)</b>	<b>HIGH (4)</b>	<b>VERY HIGH (5)</b>
	<b>Impact</b>				