Health Research Authority

Strategic Risk Register

Strategic Risks Introduction

Strategic risks are risks that could impact the achievement of an organisation's overarching objectives, such as compliance, reputation, or long-term sustainability. These risks are typically monitored by the board and senior leadership because they relate to governance, strategic priorities, and assurance processes.

In contrast, an **operational risk** is concerned with day-to-day activities and processes within the organisation, such as system failures, staff shortages, or procedural errors. Operational risks are managed at departmental or service levels and focus on ensuring smooth delivery of services and internal controls. In short, strategic risks are high-level, while operational risks are tactical and linked to routine operations.

The HRA strategic risks are designed to provide assurance rather than serve as operational action plans. They identify sources of assurance, such as internal audits, external reviews, performance reports, and governance processes, that demonstrate whether controls are effective. Unlike operational risk action plans, which detail steps to fix issues, the strategic risks ask; How do we know the risk is being managed effectively? This shifts the emphasis from doing tasks to evidencing control effectiveness, enabling the Board to make informed decisions about whether risks are within tolerance.

Each strategic risk is assessed by the Executive Committee using a 5x5 risk matrix that evaluates both likelihood and impact. Scores are agreed collectively to ensure consistency, transparency, and a shared understanding of the organisation's overall risk position.

Within the HRA Strategic Risk Register, strategic risks are scored differently from operational risks. The HRA expresses its risk appetite through two concepts:

- **Optimal Risk Position** – The level of risk the HRA aims to operate within to meet its objectives.
- **Tolerable Risk Position** – The maximum level of risk the HRA is willing to accept.

Defining these positions provides a clear framework for decision-making. It sets out both the target level of risk and the acceptable boundaries within which the organisation can pursue its strategic objectives.

Strategic Risk Score Definitions

- **Inherent Risk** – The level of risk before any controls or mitigation are applied; the exposure that exists in an untreated state.

- **Residual Risk** – The level of risk remaining after controls or mitigation have been implemented. Some residual exposure will always remain.
- **Tolerable Risk** – The level of risk the organisation is willing to operate with, given current constraints and practical considerations.
- **Optimal Risk** – The desired level of risk, representing the most effective balance between exposure and control.

5 Catastrophic impact	**5**	**10**	**15**	**20**	**25**
4 Major impact	**4**	**8**	**12**	**16**	**20**
3 Moderate impact	**3**	**6**	**9**	**12**	**15**
2 Minor impact	**2**	**4**	**6**	**8**	**10**
1 Insignificant impact	**1**	**2**	**3**	**4**	**5**
	1 Rare likelihood	2 Unlikely likelihood	3 Possible likelihood	4 Likely likelihood	5 Certain likelihood

Strategic Risk Summary

Strategic Risk Register Summary (November 2026)

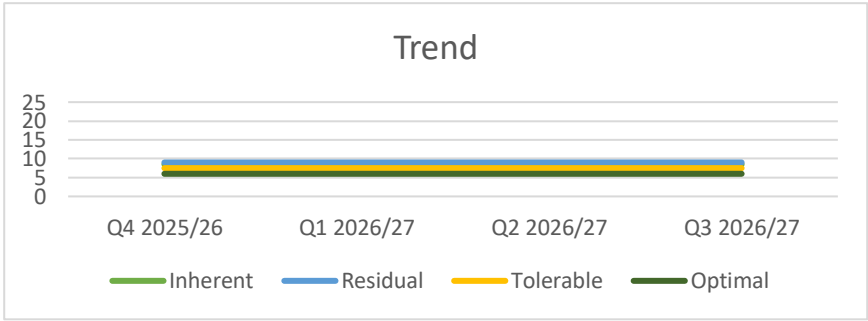
The November 2026 Strategic Risk Register records six strategic risks, based on assessments last reviewed on 6 October 2026, with the next reviews scheduled for January 2027. Five risks are at their tolerable scores: supporting UK growth in life sciences (9), helping reduce health inequalities (6), increasing the impact of money invested (12), digital (12) and resilience (12). Resources is the only risk above tolerance, with a residual score of 12 against a tolerable score of 8, reflecting funding pressures, workforce capacity and skills constraints, and competing delivery priorities. The principal cross-cutting exposures are resource adequacy, prioritisation and change delivery, digital infrastructure and cyber security. Recorded improvements focus on strategy oversight, governance structures, productivity and efficiency, the target operating model and strategic workforce planning. Resilience is assessed at tolerance, with controls covering cyber prevention, detection, response and recovery, including supplier security.

Risk	Strategic objective / theme	Executive lead	Residual score	Tolerable score	Current position	Key oversight focus
1.1 Supporting UK growth in life sciences	Support growth in life sciences	CEO	9	9	At tolerance	Strategy delivery, RSP and stakeholder confidence; evidence of progress on the planned Change Delivery and Governance Delivery Groups and meeting-structure review.
2.1 Helping reduce health inequalities	Help reduce health inequalities	CEO	6	6	At tolerance	At optimal score as well as tolerance; assurance through equality impact assessments, community engagement and performance reporting, alongside the recorded strategy governance improvements.
3.1 Increasing	Increase the impact of public	CEO	12	12	At tolerance	Productivity, efficiency, prioritisation and value for money; evidence that

the impact of money invested	investment in research					planned strategy governance changes address the recorded oversight gaps. Optimal score: 8.
4.1 Digital	Digital capability supporting all strategic priorities	Chief Digital Transformation Officer	12	12	At tolerance	Digital transformation, legacy-system stability, delivery capacity and data governance. Control-gap and assurance-improvement fields are blank, limiting visibility of any outstanding improvements. Optimal score: 8.
5.1 Resources	Financial and people resources supporting strategic delivery	Deputy Chief Executive and Director of Resources	12	8	Above tolerance	Funding and workforce capacity; progress on strategy delivery plans, the productivity and efficiency framework, cultural transition, target operating model and strategic workforce planning. Tolerable and optimal scores: 8.
6.1 Resilience	Cyber security, and organisational resilience	Chief Digital Transformation Officer	12	12	At tolerance	At tolerance, but above the optimal score of 8. Assurance on cyber prevention, detection, response and recovery, including access controls, vulnerability management, supplier security, incident exercises and backup restoration; improvement-plan and assurance-gap fields remain blank.

Strategic - 1.1 Supporting UK growth in life sciences

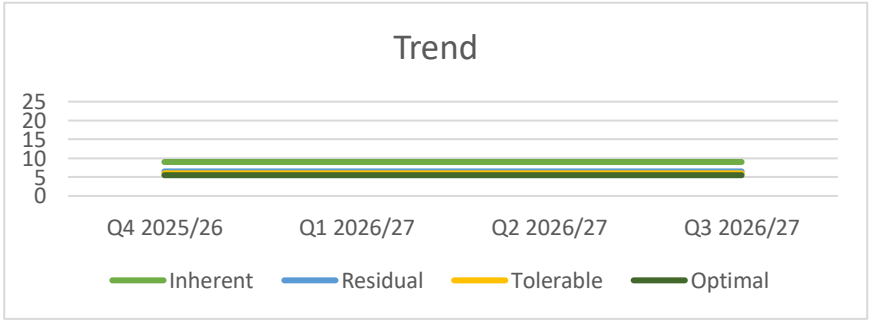
Risk Summary	The HRA's strategy is to make the UK the easiest place in the world to do excellent health and social care research that people can trust, helping grow the contribution of life sciences to our economy.
Principal Risk	The **Health Research Authority (HRA)** may fail to deliver on its objective to support growth in life sciences, it faces several strategic and operational risks across its core mission areas. **Cause:** • Inadequate digital infrastructure • resource constraints • policy misalignment • cybersecurity and data governance • stakeholder confidence. **Effect:** • Slower production of research evidence and in turn, the development and approval of new treatments and technologies, or adoption of new standards • loss of investment • erosion of trust • negative perception of the UK's research environment • failure to meet government priorities • disconnect between policy and practices • reduced funding opportunities • inefficient use of public resources.
Strategic Objective	Support growth in life sciences
Lead Committee	Executive Committee
Executive Lead	CEO

Initial Date of assessment	12/02/2026
Last reviewed	06/10/2026
Next review	January 2027
Previous Strategic Risk	• HRA is unable to deliver transformed RSP to meet the requirements of the health research community and support the vision of the HRA. • Trust of research participants and the public is lost in research and HRA.
Risk Appetite	**Strategy – Open**: Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2–3-year intervals.
Inherent Risk Score (Likelihood x Impact)	3x3=9
Residual Risk Score (Likelihood x Impact)	3x3=9
Tolerable Risk Score (Likelihood x Impact	3x3=9
Optimal Risk Score (Likelihood x Impact)	2x3=6
Risk Trend	

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• HRA Strategy 2025-28 • Corporate Portfolio Office (CPO) to help and support the HRA to do the right projects and programmes, in the right way, at the right time. • Performance Monitoring • Risk Appetite Statement • RSP	• Strategy Development Oversight.	• Introduction of Change Delivery Group • Introduction of Governance Delivery Group	• Board • Executive Committee • Portfolio Delivery Group • Staff Survey • Performance Dashboards • Audit & Risk Committee • RSP Board • Risk & Compliance Monitoring • Audit Reviews (GIAA) • Board Assurance Reports	• Strategy Governance Forum	• Review meeting structures

Strategic - 2.1 Helping reduce health inequalities

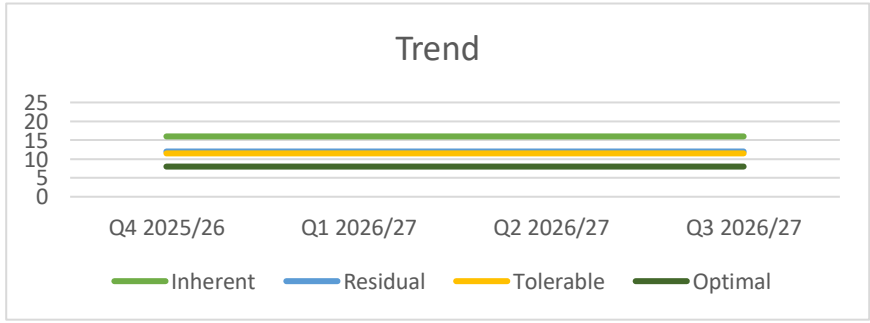
Risk Summary	The HRA strategy aims to ensure that health and social care research is done with and for everyone. Meaning that we can all benefit from the research findings, helping reduce health inequalities.
Principal Risk	The **Health Research Authority (HRA)** may fail to deliver on its objective to help reduce health inequalities, it faces several strategic, reputational, and operational risks. **Cause:** • Lack of inclusivity in research policy (funding, priorities, etc) and research design and conduct • misalignment with national health priorities • insufficient collaboration • perceived bias or inequality • lack of transparency **Effect:** • Reinforcing or Widening disparities in health outcomes • reduced access to inclusive research • missed opportunities • loss of credibility • perception of institutional bias or exclusion • criticism from advocacy groups • reduced influence.
Strategic Objective	Help reduce health inequalities
Lead Committee	Executive Committee
Executive Lead	CEO
Initial Date of assessment	12/02/2026
Last reviewed	06/10/2026

Next review	January 2027
Previous Strategic Risk	• The HRA risks making decisions that do not take account of a diverse range of views and undermines its effectiveness in meeting its public sector equality duty. • Trust of research participants and the public is lost in research and the HRA.
Risk Appetite	**Strategy – Open**: Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2–3-year intervals.
Inherent Risk Score (Likelihood x Impact)	3x3=9
Residual Risk Score (Likelihood x Impact)	2x3=6
Tolerable Risk Score (Likelihood x Impact	2x3=6
Optimal Risk Score (Likelihood x Impact)	2x3=6
Risk Trend	

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• HRA Strategy 2025-28 • Equality Impact Assessments • Risk Appetite Statement • Community Committee • Corporate Portfolio Office (CPO) to help and support the HRA to do the right projects and programmes, in the right way, at the right time.	• Strategy Development Oversight	• Introduction of Change Delivery Group • Introduction of Governance Delivery Group	• Board • Executive Committee • Audit & Risk Committee • Community Committee • Impact Assessments • Performance Dashboards • Audit & Risk Committee • Risk & Compliance Monitoring • Audit Reviews (GIAA) • Board Assurance Reports	• Strategy Governance Forum	• Review meeting structures

Strategic - 3.1 Increasing the impact of money invested

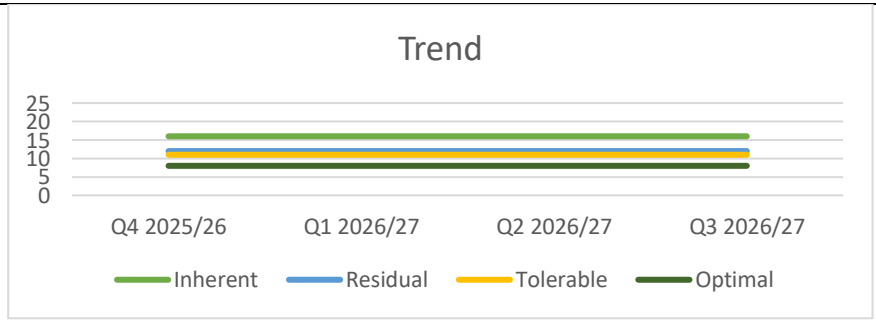
Risk Summary	The HRA through its strategy and work ensure the health and social care research system is streamlined, efficient and encouraged and supports success, increasing the impact of investment.
Principal Risk	The Health Research Authority (HRA) may fail to deliver on its strategic objective of increasing the impact of money invested in health and social care research, it faces a range of strategic, reputational, operational, and systemic risks. **Cause:** • Failure to embed inclusivity • insufficient acceleration of research processes • digital transformation challenges • transparency and reporting gaps • public confidence disparities • fragmented research ecosystem • policy and regulatory shifts. • Lack of a cohesive approach to efficiency and productivity including prioritisation and reporting **Effect:** • Reduced value for public investment • failure to meet national health priorities • loss of public trust • stakeholder disengagement • wider impact on UK research competitiveness • policy and regulatory setbacks. • Unable to demonstrate HRA value to the public purse
Strategic Objective	Increasing the impact of money invested in health and social care research

Lead Committee	Executive Committee
Executive Lead	CEO
Initial Date of assessment	12/02/2026
Last reviewed	06/10/2026
Next review	January 2027
Previous Strategic Risk	• HRA is unable to deliver transformed RSP to meet the requirements of the health research community and support the vision of the HRA.
Risk Appetite	**Strategy – Open**: Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2–3-year intervals.
Inherent Risk Score (Likelihood x Impact)	4x4=16
Residual Risk Score (Likelihood x Impact)	3x4=12
Tolerable Risk Score (Likelihood x Impact	3x4=12
Optimal Risk Score (Likelihood x Impact)	2x4=8
Risk Trend	

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• HRA Strategy 2025-28 • Corporate Portfolio Office (CPO) to help and support the HRA to do the right projects and programmes, in the right way, at the right time. • Performance Monitoring • Risk Appetite Statement • Risk Management Systems	• Strategy Development Oversight.	• Introduction of Change Delivery Group • Introduction of Governance Delivery Group	• Board • Executive Committee • Portfolio Delivery Group • Staff Survey • Performance Dashboards • Audit & Risk Committee • RSP Board • Risk & Compliance Monitoring • Audit Reviews (GIAA) • Board Assurance Reports	• Strategy Governance Forum	• Review meeting structures

Strategic - 4.1 Digital

Risk Summary	The HRA strategy outlines how it intends to achieve its core objectives. However, if the HRA lacks suitable and sufficient digital infrastructure - particularly systems capable of supporting integrated research application processes - it may be unable to deliver on its three strategic priorities: driving UK growth in life sciences, reducing health inequalities, and maximising the impact of public investment in research. Robust and scalable digital systems are therefore essential to enabling effective delivery and sustaining long-term strategic momentum.
Principal Risk	If the Health Research Authority (HRA) does not have digital systems that are both suitable and sufficient - particularly in supporting integrated research application processes - it may be unable to effectively deliver its strategic objectives. These include driving UK growth in life sciences, reducing health inequalities, and maximising the impact of public investment in research: **Cause:** • Legacy infrastructure • underinvestment in digital transformation • skills and capacity gaps • sub-optimal change management • cybersecurity and data governance risks. **Effect:** • Slower research approvals • missed opportunities • barriers to inclusive research • delayed insights • limited public engagement • inefficient use of resources • poor data visibility

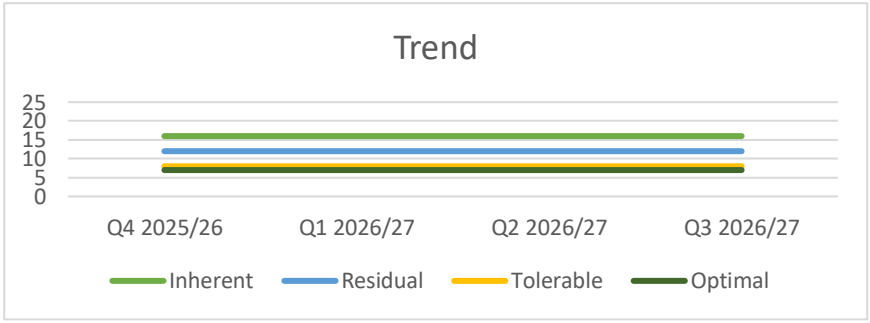
	• reduced transparency
Strategic Objective	Driving UK growth in life sciences. Reducing health inequalities. Maximising the impact of public investment in research
Lead Committee	Executive Committee
Executive Lead	Chief Digital Transformation Officer
Initial Date of assessment	12/02/2026
Last reviewed	06/10/2026
Next review	January 2027
Previous Strategic Risk	• HRA is unable to deliver transformed RSP to meet the requirements of the health research community and support the vision of the HRA. • Level of stability and maintainability of BGO Systems legacy infrastructure decreases and further incidents and issues with legacy systems may occur during any remedial work and upgrade in hardware.
Risk Appetite	**Technology – Open**: Systems / technology developments considered to enable improved delivery. Agile principles may be followed.
Inherent Risk Score (Likelihood x Impact)	4x4=16
Residual Risk Score (Likelihood x Impact)	3x4=12
Tolerable Risk Score (Likelihood x Impact	3x4=12
Optimal Risk Score (Likelihood x Impact)	2x4=8
Risk Trend	

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• HRA Strategy 2025-28 • Stakeholder engagement • Risk Appetite Statement • Training • Business Continuity Systems • Data Governance & Security • Continuous improvement			• System Performance Dashboards • Risk Monitoring • Audits • Board Assurance Reports • Stakeholder Feedback		

Strategic - 5.1 Resources

Risk Summary	The HRA strategy outlines how it intends to achieve its core objectives. However, if the HRA lacks appropriate financial and human resources, it may be unable to deliver on its three strategic priorities: supporting UK growth in life sciences, reducing health inequalities, and increasing the impact of public investment in research. Ensuring resource adequacy is therefore critical to maintaining momentum and achieving meaningful outcomes.
Principal Risk	The Health Research Authority (HRA) may fail to deliver on its strategic objectives if appropriate resources either financial or people are not available. **Cause:** • Reduced government funding • increased operational cost (e.g. unfunded pay awards, NI costs, digital investment) • competing and growing national priorities resulting in increased strategic portfolio • People (employed staff and our community) capacity constraints • skills gaps • inadequate planning or prioritisation • limited flexibility. **Effect:** • Failure to achieve strategy key results and objectives • Delays in research approvals • reduced capacity to support innovation • loss of international competitiveness • limited outreach and engagement • fewer research initiatives

	• reduced ability to monitor and evaluate equity impacts • inefficient processes • weakened oversight and assurance • staff burnout and turnover • Reduced community engagement • backlogs in approvals • inability to modernise systems • loss of trust • perception of inefficiency or ineffectiveness • reduced influence.
Strategic Objective	Supporting UK growth in life sciences. Reducing health inequalities. Maximising the impact of public investment in research.
Lead Committee	Executive Committee
Executive Lead	Deputy Chief Executive and Director of Resources
Initial Date of assessment	12/02/2026
Last reviewed	04/11/2026
Next review	January 2027
Previous Strategic Risk	• The HRA risks making decisions that do not take account of a diverse range of views and undermines its effectiveness in meeting its public sector equality duty. • The HRA may not be able to deliver its objectives due to financial pressures. • The HRA is unable to recruit or retain an effective workforce due to the current employment market. • Organisational Design (OD) is a fundamental part of what makes an organisation successful and focuses on aligning the shape and structure of an organisation with its strategy. Inadequate OD may result in the organisation not meeting agreed objectives and failure to deliver projects and programmes.

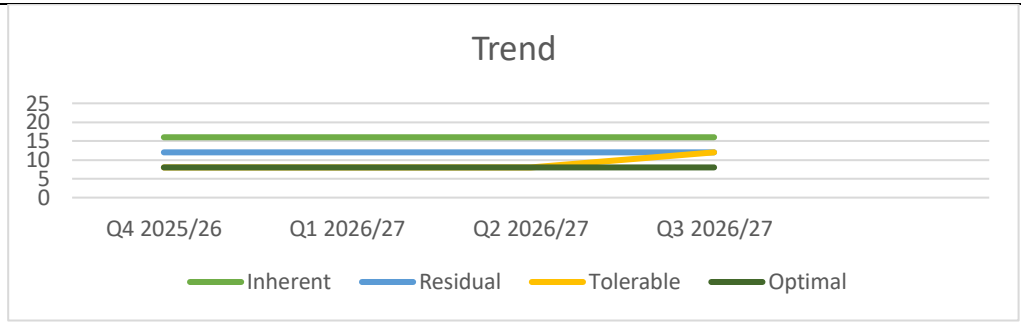
	• The organisation has limited capacity to deliver all Statute responsibilities, business as usual operations, DHSC and external expectation, as well as deliver RSP. This risk will increase in likelihood and impact given the current fiscal environment.
Risk Appetite	**Financial – Minimal**: Only prepared to accept the possibility of very limited financial impact if essential to delivery. **People – Cautious**: Seek safe and standard people policy. Decision making authority generally held by senior management.
Inherent Risk Score (Likelihood x Impact)	4x4=16
Residual Risk Score (Likelihood x Impact)	3x4=12
Tolerable Risk Score (Likelihood x Impact	2x4=8
Optimal Risk Score (Likelihood x Impact)	2x4=8
Risk Trend	

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• Financial management internal controls in place • Business planning process in place • People Strategy • Financial Strategy • Risk Management Systems • Spend controls • Financial reporting to DHSC • Efficiency reporting to DHSC	• Delegated strategy delivery • ExCo prioritisation • Cultural change to enable strategy (TOM) • Mature strategic workforce planning	• Strategy delivery plans • Productivity and efficiency framework • Culture definition and transition plan • Design and implementation of the target operating model (TOM) • Strategic workforce planning developing closely aligned to business planning	• Internal audit • External audit • Functional standards review • Audit and Risk Committee • Board • Accountability meetings	• Consolidated view of level of risk across financial and people • Possible insufficient data and evidence of workforce capacity and capability • Unclear resilience testing of TOM design until delivered in 2027 onwards • Clarity of data centralisation on HRA resource	• Joined up resourcing panel and introduction of scrutiny at Recruitment Panel to align priorities • Developed workforce planning against business planning in 2027/2028 round • Corporate alignment of reporting against controls and action plans

Strategic - 6.1 Resilience

Risk Summary	The HRA depends on secure, reliable digital systems and information to deliver its strategic objectives. If its cyber security arrangements do not keep pace with evolving threats, vulnerabilities and increasing reliance on digital services, a successful cyber-attack could compromise the confidentiality, integrity or availability of HRA information and systems. This could prevent or materially disrupt delivery of the HRA's three strategic goals: supporting UK growth in life sciences, reducing health inequalities, and maximising the impact of public investment in research.
Principal Risk	If the Health Research Authority (HRA) does not prevent, detect, respond to and recover effectively from a cyber-attack, unauthorised individuals may access, disclose, alter, destroy or restrict access to sensitive information and critical digital services. This could materially impair the HRA's operations, regulatory responsibilities and ability to achieve its strategic objectives. **Causes:** • Exploitation of unpatched, unsupported or misconfigured systems. • Phishing, credential theft or other social-engineering attacks. • Weak identity and access management, including excessive privileges. • Inadequate security monitoring, threat detection or incident response capability. • Compromise of third-party suppliers or technology services. • Insufficient staff awareness of cyber security responsibilities. • Inadequate cyber investment, governance, secure configuration, backup protection or recovery testing. **Effects:** • Unauthorised access to, disclosure of, alteration of or loss of personal, commercially sensitive or operational information.

	• Loss of availability or integrity of critical systems and data, disrupting research approvals and oversight. • Harm to data subjects and research stakeholders. • Regulatory breach, including non-compliance with UK GDPR, with potential enforcement action, fines or legal liability. • Financial loss and increased recovery costs. • Loss of public, partner and stakeholder trust, adverse media coverage and reputational damage. • Reduced staff capacity and morale, and impaired delivery of the HRA's strategic objectives.
Strategic Objective	Supporting UK growth in life sciences. Reducing health inequalities. Maximising the impact of public investment in research
Lead Committee	Executive Committee
Executive Lead	Chief Digital Transformation Officer
Initial Date of assessment	12/02/2026
Last reviewed	06/10/2026
Next review	January 2027
Previous Strategic Risk	• The HRA's operational delivery is seriously compromised by a Cyber-attack resulting in commercially sensitive / personal data being accessed, or access being restricted to HRA digital systems by unauthorised individuals.
Risk Appetite	**Security – Minimal:** Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures.
Inherent Risk Score (Likelihood x Impact)	4x4=16
Residual Risk Score (Likelihood x Impact)	3x4=12
Tolerable Risk Score (Likelihood x Impact	3x4=12
Optimal Risk Score (Likelihood x Impact)	2x4=8

Risk Trend	

Trend
25
20
15
10
5
0
Q4 2025/26
Q1 2026/27
Q2 2026/27
Q3 2026/27
Inherent
Residual
Tolerable
Optimal

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
• Annual completion of the Data Security and Protection Toolkit, with identified gaps tracked through a formal improvement plan. • Information Governance Steering Group oversight of cyber security, information governance risks, incidents and control effectiveness, with escalation through the HRA's governance structure. • Defined cyber security policies, standards and accountabilities, supported by regular risk assessment and compliance review. • Identity and access controls, including least-privilege access, timely joiner/mover/leaver processes,	• Identified and reviewed through DSP Toolkit assurance, cyber risk assessments, vulnerability and security monitoring, incident and near-miss reporting, supplier assurance, internal audit findings and relevant threat intelligence.		• Annual Data Security and Protection Toolkit submission and improvement-plan monitoring. • Information Governance Steering Group review of cyber risks, incidents, control performance and remediation actions. • GSG annual reporting to the Audit and Risk Committee. • Independent internal audit and periodic technical assurance, including vulnerability assessment and penetration testing where proportionate. • Evidence from access reviews, patch and vulnerability reporting, security monitoring,		

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
privileged-access management and multi-factor authentication where supported. • Patch, vulnerability and secure-configuration management for systems and devices. • Endpoint, email and network security controls, with logging, monitoring and escalation of suspicious activity. • Mandatory cyber awareness training and phishing education for staff. • Cyber incident response procedures, roles and escalation routes, tested through exercises and lessons learned. • Protected backups and restoration testing for critical systems and information. • Cyber security due diligence,			backup restoration tests and cyber incident exercises. • Assurance over key suppliers through due diligence, contract management and service reviews. • Compliance review against applicable government functional standards, regulatory requirements and HRA policies."		

Controls	Gaps in Controls	Plans to improve control	Sources of assurance	Gaps in assurance	Plans to improve assurance
contractual requirements and ongoing assurance for key suppliers and hosted services."					