Report to: Audit & Accounts Committee Meeting: 8th July 2026

Director or Business Manager Lead: Matthew Finch – Communities and Environment

Lead Officer: Richard Bates – Health, Safety, Risk and Insurance Manager

Report Summary	
Report Title	Strategic Risk Management
Purpose of Report	To provide an update to members highlighting the Council's 2026/27 Strategic Risk Register and its current status.
Recommendations	Members of the Committee are asked to note amendments to the Strategic Risk Register and to highlight any issues of concern.
Reason for Recommendation	To ensure Committee members are aware of the new 2026/27 risk register and performance of the previous Council's strategic risks.

1.0 Background

1.1 Risk Management is the process of identification and management of risks faced by the Council, which have the potential to significantly prevent it from achieving its key/agreed objectives. Proactively identifying potentially significant risks and implementing suitable control strategies help prevent these risks from being realised, or if this is not possible, to mitigate the risk to a tolerable level.

1.2 Strategic risks are those risks that have the potential to halt or significantly interfere with the ability of the Council to achieve its core objectives, priorities and/or ambitions. Those risks that have the potential to halt or interfere with the ability of business units to achieve their specific operational service priorities are detailed with the operational risk register.

1.3 The previous 2025/26 strategic risk register was last reviewed by Members in December 2025.

2.0 Strategic Risk Review – New register 2026/27

2.1 In accordance with the Risk Management Policy, a facilitated strategic risk workshop was undertaken with the Senior Leadership Team (SLT) in February 2026. This workshop evaluated all existing strategic risks and identified emerging risks for the forth coming year.

Undertaking annual strategic risk reviews helps identify significant potential challenges the council may face so it may appropriately control or mitigate as required and where possible. The purpose of the annual strategic risk workshop is to:

a) Consider the suitability of the existing register,
b) Identify new, emerging or future significant risks, and
c) Develop a formal register to address these risks

2.2 During the workshop, SLT agreed that:

a) 3 existing strategic risks should be retained,
b) 5 strategic risks would be reassigned as operational risks, and
c) 3 new strategic risks be developed.

Details of these changes are listed below.

NEW STRATEGIC REGISTER 2026/27		
NEW RISK	**Description**	**SLT OWNER**
SR601 Finance GF	Financial Sustainability- General Fund	Nick Wilson
SR602 Finance HRA	Financial Sustainability- HRA	Nick Wilson & Suzanne Shead
SR603 DATA	Data Management Security	Nick Wilson
NEW- SR604 Housing Compliance	Housing Statutory Compliance Management	Suzanne Shead
NEW – SR605 Major projects	Delivering Major Projects	Matt Lamb
NEW -SR606 LGR	LGR Transition	Deborah Johnson

RISKS REMOVED FROM THE STRATEGIC REGISTER	
Risk	**Notes**
SR503 Failure to achieve housing growth targets	Reviewed and converted to an operational risk. Now reflects the operational issues regarding planning targets, DPP and their effect on the planning team.
SR504 Contract/Supply Failure	Reviewed and converted to an operational risk. Re focussed to specifically address housing contract functions.
SR505	Reviewed and converted to an operational risk.

Workforce	Merged with existing HR ORs relating to workforce.
SR506 Governance	Reviewed and converted to an operational risk. New operational risk owned by the Monitoring Officer. Financial elements (i.e. fraud) now located within Fraud risk register.
SR508 Environment	Reviewed and converted to an operational risk. Aligned with Corporate Carbon group's action plan.

2.3 Only 3 of the current strategic risks (SR601, SR602 and SR603), identified within the 26/27 register are pre-existing and without alteration/amendment. These therefore are fully developed and have established action plans.

2.4 SR604, SR605 and SR606 are new risks. These have all been fully reviewed and developed to ensure they are appropriate and have suitable action plans. These developed risks have been to SLT for discussion/agreement and are now active.

2.5 All strategic risk identified within the 26/27 register are owned by a member of SLT. Risk owners, with the assistance of lead officers and Safety, Risk and Insurance Manager, meet on a quarterly basis to review and develop the risk.

3.0 Strategic Risk Register Performance

3.1 All strategic risks have identified actions. The purpose of these actions is to mitigate the risk to a tolerable level. Actions and due dates are determined by the risk owner and their progress is monitored at quarterly reviews.

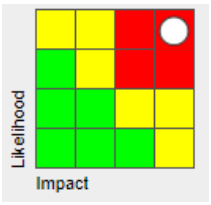
3.2 Due to the nature of strategic risks some actions are assigned long due dates, many of which may exceed a year before completion is required. Other actions may also be cyclical and appear a number of times within a year.

3.3 The current strategic risk register has a total of **54** active actions assigned to the 6 risks. The table below illustrates the current status of each strategic risk score and their associated actions.

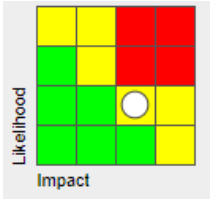
The actions progress bar provides information relating to the total number of actions assigned to each risk for the previous year and their current status i.e. completed, in progress or overdue.

SR601- Financial Sustainability- General Fund

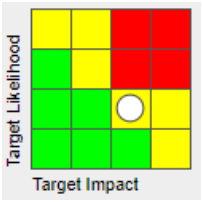
Uncontrolled Risk



Current Risk Score

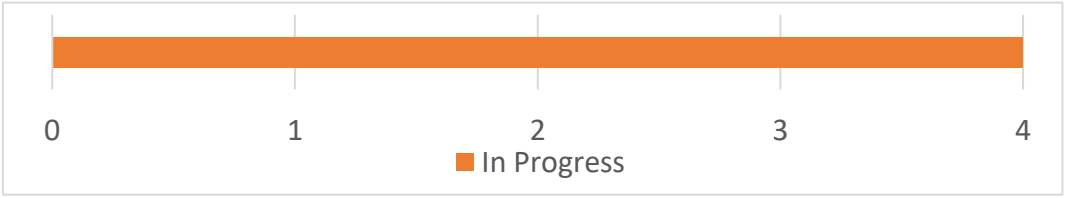


Target Risk Score



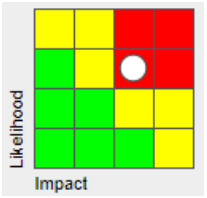
- Risk score has remained static.
- At SLT target score.

Actions – Progress

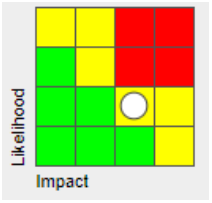


SR602 - Financial Sustainability- HRA

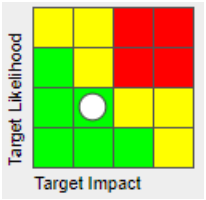
Uncontrolled Risk



Current Risk Score

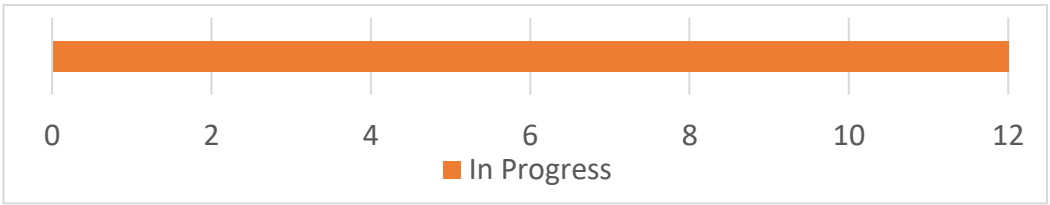


Target Risk Score



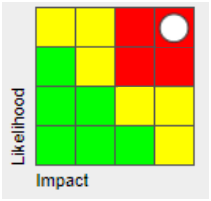
- Risk score has remained static.
- Not yet at SLT target score.

Actions – Progress

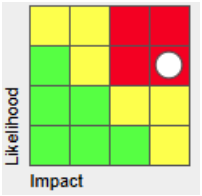


SR603- Data Management Security

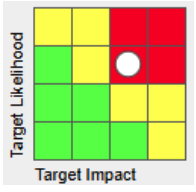
Uncontrolled Risk



Current Risk Score

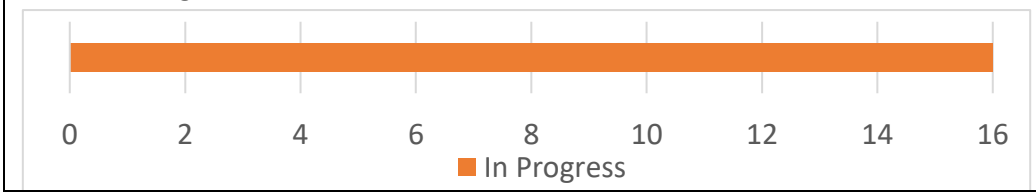


Target Risk Score



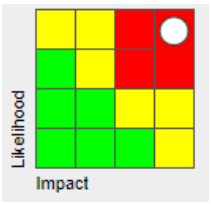
- Risk score has remained static.
- Not yet at SLT target score.

Actions – Progress

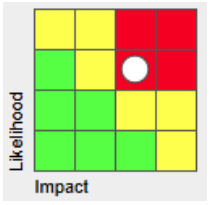


SR604 – Housing Statutory Compliance Management

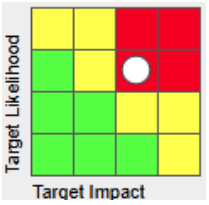
Uncontrolled Risk



Current Risk Score

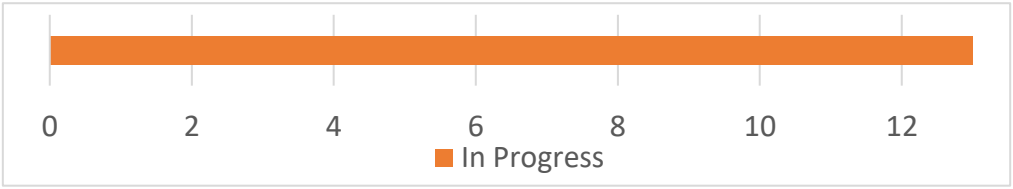


Target Risk Score



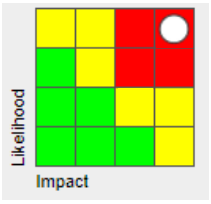
- New risk.
- At SLT target score.

Actions – Progress

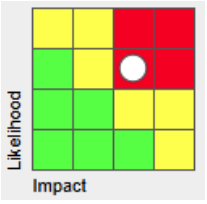


SR605 – Delivering Major Projects

Uncontrolled Risk



Current Risk Score

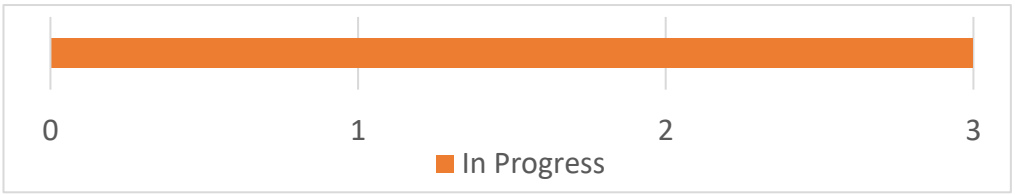


Target Risk Score

To be confirmed at next review

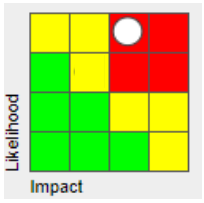
- New risk
- Target score to be confirmed.

Actions – Progress

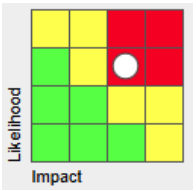


SR606- LGR

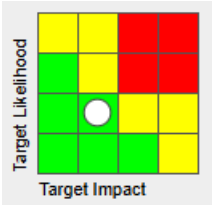
Uncontrolled Risk



Current Risk Score

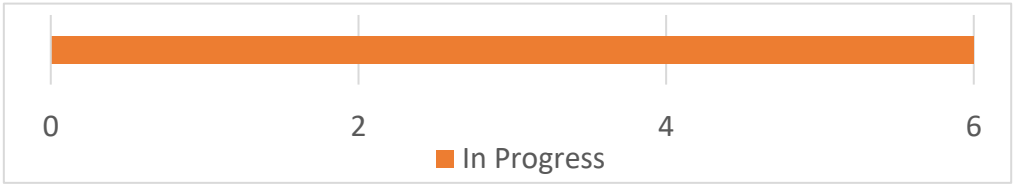


Target Risk Score



- New risk.
- Not yet at SLT target score.

Actions – Progress



3.0 Strategic Risk Register 2026/27- Development and Review

3.1 All strategic risks continue to be reported to SLT, via our agreed assurance process, on a quarterly basis. The purpose of this process is to identify those risks that are red, failing or not reviewed during the previous quarter, for consideration by SLT.

3.4 All 6 current strategic risk assessments have been appended to this report in full.

4.0 Proposal/Options Considered

4.1 Members of the committee note the amendments to the Strategic Risk Register. An update report will be brought to the Audit and Governance Committee in 6 months.

5.0 Implications

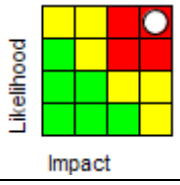
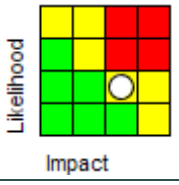
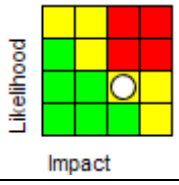
In writing this report and in putting forward recommendation's officers have considered the following a range of implications. This report in itself does not have any implications. During the risk reviewing process any controls that are identified are considered in terms of the implications they may have before they are agreed as an appropriate control.

Background Papers and Published Documents

None for this report

APPENDIX 1 – Strategic Risks

SR601 Financial sustainability – General Fund	
Description	Ensuring financial sustainability of the general fund to allow the council to undertake its core functions, deliver services, meet its corporate priorities and objectives.
Lead Officer	Nick Wilson
Support Officers	

Uncontrolled Risk Matrix	Current Risk Matrix	Target Risk Matrix
		

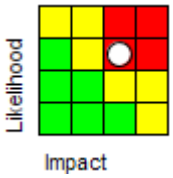
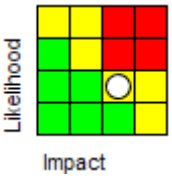
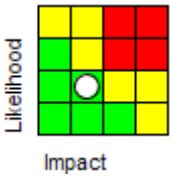
Date Last Reviewed
02-Mar-2026

Controls In Place	Quarterly Capital monitoring meetings Investments approved in line with the annually agreed Treasury Management Strategy Annual refresh of Medium Term Financial Plan including management of reserves Council approved Capital programme Financial implications added to Committee reports by Financial Services and a unique reference given each time Financial strategies and budget reviewed through Cabinet annually Use of external Medium Term Financial Plan tool which assists with forecasting future Business Rates income for the following year budget Assigned project manager for each major project the Council is embarking on Commercial officer group established to identify business opportunities in service areas Director/Business Unit Manager quarterly meetings reviewing Directorate financial position Approved Commercial strategy to support objectives set out in the MTFP Approved Investment Plan to support the objectives set out in the Commercial Strategy Nottinghamshire Business Rates Pool mitigating large impacts of reductions in Business Rates. This is kept under review by Nottinghamshire S151 officers Quarterly budget monitoring report tabled at SLT, Cabinet and PPIC Annual Financial Regulations training in place Lead authority for administration around Notts Business rates pool Contract procedure rules in Constitution refreshed May 22 Acquisition and disposal policy - Approved Nov 2021 Internal Audit Corporate land and property group established and meet regularly Review of chancellor's budget statements/fiscal events Commercial group established and projects identified by BM's across the authority. Allocation of resources both staffing and financial to account the councils'

	major projects in the capital programme and in the pipeline. Initial allocation of resources carried out by SLT. Fair funding 2.0 review no completed future 3 year funding agreed MTFP annual shortfall review complete to be reviewed again 4th year

Risk Categories	Financial Meeting corporate objectives Service delivery Reputation Governance Compliance
Trigger/Event	Unforeseen rise in interest rates over forecasted levels Changes in national policy eg. fair funding review, change to government political parties Change in local political balance resulting in change in priorities Banking crisis Over reliance and poor decision making on investments Member priorities diverging from corporate priorities Increase CPI/RPI figures Failure of subsidiary companies Major contract failure Failure of HRA Reduction in Business Rates Poor decision making and business planning Budgeted income levels not meeting target Actual funding received not in line with expected funding (central Gov and Notts Pool) Change in government policy significantly reducing income/funding Changes in government policy/direction impacting resulting in additional costs Failure in compliance/ governance Fraud Global Pandemic Economic downturn Cyber-attack/fraud Utility price increase Supply chain – significant sudden increase in costs Levelling up Nottingham and Nottinghamshire project Local government reorganisation
Impact	Inability to fund services resulting in reduction in discretionary services and reduction in quality-of-service provision Inability to meet corporate priorities/community plan Inability to meet legislative requirements External auditors review Government taskforce Negative media/reputation Loss of ability to make local decisions Division between members and officers Greater division between political parties Staff morale, loss of key staff and reduction in workforce Staff morale and loss of key staff Fines/ enforcement S151 officer issues S114 notice Curtailment of activities of the subsidiaries/HRA/Major projects Impact on residents and communities Impact on income streams Reduction/disposal of assets Impact on the funding of the capital programme requiring reprioritisation of projects and a consequential impact on the GF due to additional interest cost/additional costs of borrowing

SR602 Financial sustainability - HRA	
Description	Financial sustainability of the HRA to ensure the council is able to provide, maintain and develop its housing stock.
Lead Officer	Nick Wilson, Suzanne Shead
Support Officers	Andrew Snape, Jordan Hempenstall, Wayne Fox, David Price, Julie Davidson

Uncontrolled Risk Matrix	Current Risk Matrix	Target Risk Matrix
		

Date Last Reviewed
17-Mar-2026

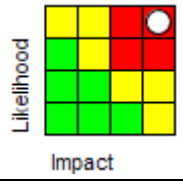
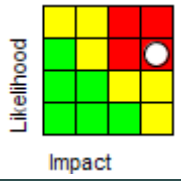
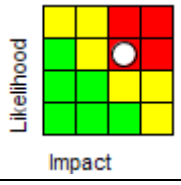
Controls In Place	• Quarterly Capital monitoring meetings • Investments approved in line with the annually agreed Treasury Management Strategy • Annual refresh of HRA financial business plan • Council approved Capital programme • Financial implications added to Committee reports by Financial Services • Financial strategies and budget reviewed through Cabinet annually • Use of external HRABP tool allows scenario planning • Assigned project manager for each major project the Council is embarking on • Director/Business Unit Manager quarterly meetings reviewing Directorate financial position • Quarterly budget monitoring report tabled at SLT and Cabinet • Annual Financial Regulations training in place • Current development programme ensuring growth in house numbers, over and above the offsetting disposals through Right to Buy • Attendance at Housing related horizon scanning events, in order to feed future impacts into HRABP • Reserves in place • Effective challenge of recharges from GF to HRA

Risk Categories	Financial Meeting corporate objectives Service delivery Reputation Governance Regulation Compliance
Trigger/Event	Change in national policy & legislative requirements Increase in interest rates Increased rent arrears Suitability of stock meeting future standards Increase or change in standards required

	Current stock does not meeting housing needs Workforce issues Failing to ensure compliance with relevant legislation causing regulatory bodies to intervene Non-compliance with RSH regulatory standards Meeting tenant priorities Ineffective strategic decision making and business planning Key HRA major projects failure Ineffective management of housing maintenance function Loss of critical income streams Fraud Failure to manage critical income streams/ invest Global Pandemic Supplier/contractor cost increases due to demand/supply issues changes in the economy Inability to secure sufficient external funding to regenerate existing stock to meet enhanced standards Conflicting strategic direction and lack of regular review of 30 year business plan Zero carbon works identifies significant increase in costs Stock condition survey identifies significant increases in costs Local government reorganisation
Impact	Inability to maintain stock to acceptable level including development of future homes Changes in national policy requiring internal funding above levels sustainable within business plan. Increased requirement to use internal funding, Reprioritisation of service delivery Cash reserves used to right off rent arrears and voids Substandard housing stock Loss of morale and high staff turnover Fines, notices, court cases and legal fees Moratorium of services Stakeholder Dissatisfaction with service delivery Greater scrutiny on service slowing decision making Poor local housing policy Project failure Contract disputes S151 officer issues S114 notice Failure to service debt Legislative requirements not met Negative impact on residents and tenants Increase in void properties Regulatory notice Loss of access to grant funding

SR603 Data management and security	
Description	Deliberate or unintentional loss/disclosure of personal, sensitive, confidential, business critical information or breach of information governance legislation
Lead Officer	Nick Wilson
Support Officers	Dave Richardson, David Clarke, Lisa Ingram

Uncontrolled Risk Matrix	**Current Risk Matrix**	**Target Risk Matrix**

Date Last Reviewed
05-Mar-2026

Controls In Place	**<u>Policy and Guidance</u>** Policy suite and supporting guidance including: ISMS Cyber security strategy IG strategy **<u>Training/ Guidance</u>** • Training for all staff taking payments in line with PCI-DSS requirements. • Training for ICT staff. • Data protection training including a section on information security and targeted training ongoing for staff located elsewhere and forms part of the induction process. • Information governance check on furniture that is being disposed of. • Information E Training completed by all staff. • Annual review of Information Asset Register. • Annual mandatory GDPR, cyber and spear phishing online training for all staff and councillors. • Guidance and training available for elected members. • Guidance on security breach procedures for Business Managers as Information Asset Owners • Data security communications to all staff following identification of risk • All data protection/ICT issues captured within single register • 6 monthly testing exercise undertaken with users- data reported to SLT & CIGG **<u>Governance and Compliance</u>** • CIO/SIRO/DPO appointed • Compliance with the government's security arrangements. • PSN compliant data & internet connections implemented • Compliance with new Cabinet Office email standards achieved. • Weekly review of ICO guidance. • Periodic PCI/DSS compliance checks • Data Privacy Impact Assessment. • Annual SIRO audit. • Review of policies and procedures to ensure compliance with latest Payment Card Industry- Data Security Standard (PCI-DSS) • Cyber Security now standing agenda item on monthly business unit management meetings. • Governance arrangements established through CIGG with monthly review. • CIGG meeting every quarter to review risks. • External Audit on ICT security annually. • Implementation of an ISMS project team • Implementation of continual assurance programme following implementation of ISMS • Amalgamation of digital transformation board with CIGG

	• CAF ready status achieved • Report template has been amended to include data protection/ICT issues **<u>ICT/Equipment specific controls</u>** Encryption for mobile devices. • Google Authenticator. • Quarterly ICT security checks internally. • Penetration test annually by external company - monthly scans of servers for weaknesses, monthly server updates and monthly scans of Microsoft Office and Windows. • Perimeter software • Hardening test on new virtual servers. • Documents scanned reducing the need for paper. • Secure server room. • East Midlands WARP membership • Monthly updates of Adobe products. • Program in place to ensure the continual maintenance & upgrade of the ICT environment. • Secure portal for Members to access the Extranet. • MDM (Mobile Device Management) implementation for mobile devices. • DMark, DKim SPF and TLS secure email authentication software. • Encryption for secure emails and large files for email. • Report & record all cyber-attacks/attempts and escalate to SLT where appropriate Users own devices cannot connect to network • 'Consent' tick box on appropriate forms. • Blocking of unauthorised network devices • All removal media is encrypted upon connection to systems **<u>Partners and Stakeholder specific controls</u>** • Non-disclosure agreements in place for third party access. • Use of data processing and agreements with partners. • Use of licensed confidential waste handler. • Letters sent to all third parties who process personal data on behalf of NSDC advising of additional responsibilities under GDPR and data processing agreements in place. • SOC implemented- security operation centre • Cyber incident response on retainer- CIR

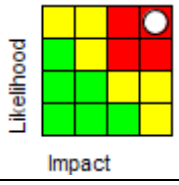
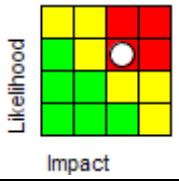
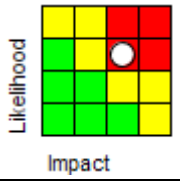
Risk Categories	Loss of vulnerable, personal, sensitive valuable data Legal compliance Reputation Financial Partners/stakeholders Disruption of service- including from a cyber attack Supply chain
Trigger/Event	**(Organisational)** • Personal, confidential or corporately sensitive/business critical information disclosed unintentionally or through error of judgement, data breach - intentional (malicious). • Theft or loss of equipment/papers/data belonging to the council, partners or third party companies. • Failure to respond to subject access requests/information requests accurately and within statutory timeframes • Failure to identify and respond to a data breach promptly and effectively • Failure to protect information from accidental loss, corruption or disclosure or other non compliance with Data Protection Principles,

	by NSDC or a third party, involving large volumes of personal data or smaller volumes of sensitive personal data • Repetition of reportable data security breach • Insufficient due diligence during procurement and termination of cloud base systems supported by third parties. • Accelerated delivery of digital agenda • Agile Working i.e. mobile/remote/home working/home printing/disposal of printed data/Outreach posts. • Loss of key resources/staff. • Reducing resources with less capacity for processing data. • New and inexperienced staff/elected members with access to data. • Lack of suitable training/competency/communications • Re-alignment and integration of new services • Misinformation/ Disinformation? **(Systems/assets)** • Cyber attack: (either targeted such as denial of service or unintentional human error e.g. - access to link on another website). • Failure to protect information assets from an internal malicious attack leading to a data breach, corruption of data assets, loss of asset or service. • Failure to adopt appropriate technical security measures for keeping data secure within our systems and platforms which results in a significant data breach • Accidental data breach through any electronic source • Use of BYOD (Bring your own device). • Unsupported software/unforeseen loss of support. • Decommissioning of property/asset **(Partners and stakeholders)** • Collaborative working, sharing, outsourcing and partnership working (including external printing and hybrid mail)/involvement in other peoples' data • Partnership working and sharing new service locations/data sharing issues. • Partner's/contractor's/host's poor data management and information security leading to data breach/loss. • Use of suppliers/third parties, etc. • Government integration agenda e.g. Increased working between public bodies • Local government reorganisation/Combined authority/change in service delivery model. • Third party access to IT systems. • Adoption of unsupported/dated systems from third parties **(Accreditations)** • Termination of PSN/GCSX standards by the Cabinet Office limiting options for securely sharing with some Public Sector organisations • Failure to comply with relevant standards and legislation including PCI-DSS/Cyber Essentials/NCSC best practice/PSN. **(External Factors)** • Emergency event-eg power loss – leading to increased reliance upon ICT systems and potential loss of data/corruption of data • Geopolitical

	(Local Government Restructure) • Increased sharing of data • Merging of systems • Integration of new systems • Capacity and resourcing shadow authority • Increase in potential cyber attacks **(AI)** • Incorrect/ unsupported use of AI • Non-compliance with DP • Non-compliance with AI policy • Inappropriate use of AI
Impact	**(Finance/legal)** • Loss/damage to an individual where the Council inappropriately released their personal data • ICO fine/Civil claims. • Resource impact of Information Commissioner investigation.eg ICO actions • Breach of Access to Information legislation bringing about financial/legal damage - imposed on the Council by the Information Commissioner and other Statutory Bodies. • Disciplinary action taken against a member of staff and elected members if a breach is found to be deliberate/malicious. **(Resource)** • Drain on resources to process and enable conformity in legislation. • Greater demand on existing resource • Operational and resource issues eg. Service interruption - where focus has to be taken away from service delivery to dealing with the breach. • Reduced service provision resulting from lack of ability to work remotely and available physical resource • Increased demand on existing services • Inability to deliver critical/key services • Capability of infrastructure/system to deliver services – i.e. increased demand during emergencies **(Reputation)** • Damage to reputation of the Council/trust by the public. • Loss of confidence within the Council • Loss of confidence with partners and stakeholders • Negative media coverage **(Partners)** • Loss of provision to customers and partners e.g. Active4Today, DWP, • CCTV (under current arrangements) leading to disputes over SLAs and contracts and potential loss of income, e.g. partner rent for Castle House. • Loss of partner data where the council is the data processor - subsequent impact on partner's reputation. • Withdrawal of service from partners and stakeholder • Cyber-attack leading to system downtime/damage/loss of data (Ransom Ware) and financial loss/ resource drain

	(Contractors/supply chain) • Less direct control over data as we procure, migrate to and terminate cloud base systems

SR604 HSG Statutory compliance management	
Description	Implementation and maintenance of suitable management systems to ensure statutory safety compliance for the "BIG 7".
Lead Officer	Suzanne Shead
Support Officers	Norman Emery, Wayne Fox

Original Matrix	**Current Risk Matrix**	**Target Risk Matrix**
		

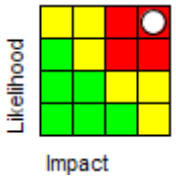
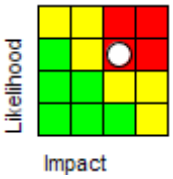
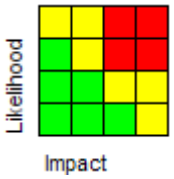
Review Date
30-Mar-2026

Controls In Place	• Policies and procedures • Dedicated Compliance team and compliance reporting procedures • Dedicated software –asset compliance/management software ICT systems • Contract management systems • Performance management systems • Training and competence Staff/tenants/contractor • Information/education to tenants • Enforcement of tenancy agreements • Assurance and scrutiny process – operational and committee levels • Use of specialist contractors/advisors • Competent/licenced/registered engineers/inspectors • Auditing and inspection processes • Reconciliation processes • Complaints processes • Tenant engagement • Maintenance/inspection programmes • Pre let inspections • Business planning • Compliance with regulatory standards • Housing Assurance Board • Safety & Quality standard self-assessment undertaken • Regular Corporate & HRA compliance shared meetings • Tenancy engagement/enforcement procedures
Risk Categories	• Legal • Negative media coverage • Reputation • Customer satisfaction/impact • Financial impact (rectification)

	• Increased resource demand
Trigger/Event	• Remedial works not undertaken in a timely manner • Poor/incomplete compliance management systems in place • Failure to undertake statutory examinations • Poor record management/ software management systems • Failure of ICT and associated support systems • Cyber-attack/Ransom ware –denied/denying access to records • Data protection loss/GDPR • Contract management – controls to manage/address poor performance/contract exit arrangements, use of evergreen contracts (non-ending), poor procurement • Poor contractor engagement • Essential supplier chain failure/goes into administration • Incorrect sub-contracting procedures • Resource demand/conflict • Recruitment – inability due to market demands • Loss of key personnel • Insufficient finance • Insufficient Resourcing • Changes in legislative/guidance requirements • Damp/mould – introduction of Social Housing Bill 2023 • Routine inspection/audit identifies non compliance • Incorrect response to an accusation, complaint or request for service • Unauthorised repairs, sabotage, maintenance, alterations and installations • Emergency incident – fire, gas, flood, preventing ability to undertake compliance tests. • Hospitalisation/fatality - Investigations to establish cause/identify reports • Local government restructure
Impact	• Loss of life/ severe injury/ hospitalisation • Service delivery - Loss of systems/equipment failure/out of use • Legal/enforcement action/Fines/Regulatory judgement Criminal procedures -Fines/enforcement action • Regulatory notice issued • Regulatory body short notice inspection • Self-referral to regulatory (co-regulation) • Diverted resources due to regulatory body investigations • Civil claim due to failure • Leaseholders litigation – communal areas, cladding and Front doors • Investigations to establish cause/identify reports for Legal/enforcement action/Fines/Regulatory judgement • Increased scrutiny/monitoring – customer, committees, Regulator etc. • Contract failure/suspension • Contract dispute • Financial – budget overspend, income generation/protection, rent loss, MTFP, viability of HRA business plan. Effect on GF income • Loss/reduction of service to Council, partners and tenants(commercial and domestic) • Financial impact (rectification) • Increased resource demand • Service delivery - Loss of essential service & System/equipment failure/out of use

	• Unable to deliver a suitable service/essential service • Need to re home tenants • Reputation • Negative local or national press coverage • Increase turnover of staff • Inability to recruit the right staff • Poor morale/stress of workforce • Political engagement • Enforcement agency engagement • Accident/incident/poisoning • Customer satisfaction/impact

SR605 Delivering Major Projects	
Description	Failure to deliver or sufficiently advance approved capital projects within the Council's Capital Programme and Community Plan prior to mandated funding deadlines and/or the end of Newark & Sherwood District Council.
Lead Officer	Matt Lamb
Support Officers	TBC

Uncontrolled Risk Matrix	**Current Risk Matrix**	**Target Risk Matrix**
		

Date Last Reviewed
24-Mar-2026

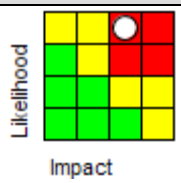
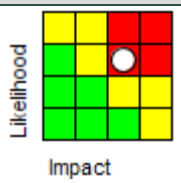
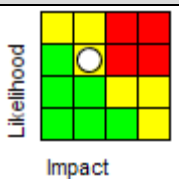
Controls In Place	• Approved capital programme • Approved community plan • Capital monitoring group • Project risk registers • Internal audits • Formal external/internal reporting including frequent reports to relevant grant funders, committees & SLT • Procurement policy • Contract procedure rules- Reference/ credit checks for suppliers prior to awarding projects • Quality based tendering process • Financial regulations • S151 officer • Credit checks • PIDs • Security of tenure including tenants - Agreement to lease upon practical completion • Dedicated and competent project managers with required skills/expertise • Delegated roles within the project team • Use of consultants where necessary • Grant funding agreements

	• Due diligence funding checks • Funding fraud risk procedures • Stakeholder engagement meetings

Risk Categories	Finance Resourcing Reputation Workforce Political Legal/Contractual Leadership Partnerships
Trigger/Event	• Overdemand • Capacity, capability, resource & Workforce issues • Loss or unavailability of key personnel/project manager • Poor governance • Finance/ budget • Market driven financial pressures (inflation, unfixed contract prices) • Procurement non-compliance • Interruptions due to incidents, unknowns & external factors diverting priority • Knock on consequences to critical path deadlines of delay • Delivery Issues/ delayed delivery (legal, approvals) • Shift in political appetite affecting project continuation or new project initiation • Delays in political decision making • Decision making from shadow authority • Changes in policy, regulations & legislation • Failure to comply with funding requirements • Grant availability & conditions • Partnership failures • Failure to comply with regulatory conditions • Supplier overload • Variations/scope creep • Lack of or inability to obtain expertise of subject exposure • Delivering partner entering administration • Third party permissions (landowners/utilities) • Limited contractor availability • Contracting • Failure to engage with stakeholders/consultees • Occupier/ end-user withdrawal or ceasing to operate
Impact	• Failure to deliver community plan/intended project objectives • Delays in delivering projects and associated benefits • Additional/repeat procurement • Alteration of initial project • Abortive work • Delivery of a project that is unsuitable or not fit for purpose • Administrative change • Additional resourcing • Capacity of staff • Decline in staff morale • Increased staff turnover • Reduced public confidence • Reputational damage & deterioration of stakeholder relationships • Misinformation/ disinformation

	• Additional financial pressures that could effect MTFP • Involvement or intervention from regulatory bodies • Fines/ prosecutions • Legal challenges • Claims against the organisation • Partners withdrawing • Withdrawal/repayment of funding • Ineligibility to apply for future funding • Negative impacts on supply chain & suppliers

SR606 LGR	
Description	To ensure smooth transition maintaining effective business as usual (BAU) delivery while implementing significant change. This includes pressures on workforce capacity, operational resilience and the ability to support staff, residents, and elected members throughout the transition
Lead Officer	Deborah Johnson
Support Officers	Carl Burns, Carina Tona, Sarah Lawrie, Nick Wilson

Uncontrolled Risk Matrix	**Current Risk Matrix**	**Target Risk Matrix**
		

Date Last Reviewed
07-May-2026

Controls In Place	**Programme Management** • Maintenance of a clear and regularly reviewed LGR programme governance structure with defined senior ownership and escalation routes. • Ongoing engagement with nationally available learning from previous LGR programmes to mitigate known risks and avoid common pitfalls. **Governance** • Governance, general purposes & LGR (GGP&LGR) committee regularly meeting and updates (council wide)

	• Internal weekly LGR meeting & weekly SLT briefing • LGR implications included within reports template **Communication and Engagement** • Proactive engagement with government • Proactive engagement with neighbouring councils and sector bodies to contribute to guidance, funding and implementation approach. • Proactive engagement with Nottingham & Nottinghamshire partner work using NSDC representation across implementation groups • Maintenance of strong, clear and consistent communication and engagement with members, staff, partners, town and parish councils and residents. • Embedded equality impact assessment and rural proofing throughout the transition and service redesign process. • Communications and Engagement Plan, agreed by all nine Councils, in place setting out clear and agreed principles, aims and objectives of the joint communications, engagement and the role of the Comms Cell • Established Comms Cell in place, with representation from all nine Councils. **Digital, Data and Technology** • Early planning for ICT, data and information governance integration, including assurance over cyber security and data protection. • Security operations centre monitoring and mitigation some cyber threats (24/7/365) • Cyber Incident Response on retainer, in case of successful cyber-attack. • Information Security Management System implemented and continual assurance on going. • Data sharing agreement in place **Capacity and Workforce** • Ensure that essential learning and development is maintained to reduce any impact on key services. • Protect BAU capacity through clear prioritisation, use of temporary resources and phased transition planning. **Financial** • Clear controls in place to manage our contracts register. • A dedicated LGR reserve to contribute to our share of the transition costs of the new authority

Risk Categories	Finance Capacity/resource Workforce Governance Reputation Service delivery
Trigger/Event	**Capacity/Workforce** • Workforce uncertainty. • Increased demand. • Loss of valued NSDC culture. • Capacity - across the entire organisation, including specific teams and individuals, resulting in resources being spread too thin.

	• Additional legislative change increasing business as usual work alongside work for LGR. • Employees experience burnout running a large change programme and maintaining BAU. • Focus and resources diverted from core compliance activity • Incomplete, inaccurate, or inconsistent staff data, including gaps in employment records. • Compressed national or regional implementation timetable reducing local capacity to plan and transition effectively. **Financial** • Financial pressures at NSDC arising from transition costs, unfunded burdens or insufficiently identified / allocated budgets to support required transition activity. • Combined financial commitments across councils not being appropriately coordinated, managed, or aligned, • Contract Register is incomplete and with incorrect details. • Contract register end dates for critical services and systems which are at the point or near the point or soon after vesting day • Non-compliance with section 24 direction. • NSDC members wanting to add new projects pre section 24. • Ineffective management of transition funds from government to support reorganisation process **Governance and Shadow Authority** • No overall control of shadow authority from May 2027 elections • Statutory officers in shadow authority do not consider the needs of each authority • Ineffective temporary governance arrangements • Failure to meet key milestones or decision deadlines, including timely approval of required documents (e.g. scheme of delegation, constitutions, committee terms of reference). • Should NSDC elections take place 2027 potential of too many new members & new administration. • Appropriate data sharing agreements are not in place or maintained throughout the transition process. • Minded to letter questions - failure to agree answers • Non agreement of representation and remit of joint committee (Pre shadow elections) • Shadow elections - failure to agree on key decision given a hung administration **Digital, Data and Technology** • Loss of clear accountability for cyber, data and digital ownership during transition. • Issues with system integrations, migrations and temporary access arrangements. • Inconsistent security controls and policies inherited from predecessor councils. • Data sharing, consolidation or unclear data controller roles. • Legacy systems and unsupported technologies Reduced cyber resilience during organisational change and competing transformation priorities. • Staff restructuring or uncertainty. • Greater focus on structural change rather than service outcomes.

	• Poor-quality or fragmented data undermining service delivery, reporting and decision-making. • Contract novation, renegotiation or inconsistent vendor management. • Inadequate funding or investment planning for future cyber, digital and data platforms. **Communication and Engagement** • Misinformation/disinformation. • Conflicting or inconsistent information from councils. • Public confusion about changes • Internal communication differences causing staff uncertainty and staff disengagement • Engagement not reaching all communities • Political narrative overtaking factual information communication • Engagement fatigue over a long programme • Reputational damage of current councils and new authorities • Lack of agreement on a single approach post decision - failure to establish a single source of the truth • Lack of adequate involvement from individual councils in the comms and engagement change programme required • Lack of understanding from individual councils on the work required from the Comms Cell as it is not an established workstream **General** • Loss of local decision-making influence at NSDC because there will be focus on shadow authority • Insufficient clarity or late changes to statutory guidance, funding or transition arrangements from central government. • External factors (flood, elections, international conflict etc.) or overdemand from emergency event • Failure to adequately consider equality, rurality or place-based impacts including what is unique about NSDC within the new structures. • Political resistance (NSDC/other authorities) • Differing priorities, capabilities and capacity across different councils • Differing levels of commitment and collaboration with other councils • Inconsistent and untimely data capturing during 'no regrets' period
Impact	**Capacity/Workforce** • Loss of key staff, with critical skills, experience and organisational specific knowledge required for transition and implementation period. • Insufficient or ineffective consultation with staff, including failure to meet agreed consultation timelines or processes. • Breakdown in trade union consultation, including failure to reach agreement where required or unresolved disputes escalating. • Failure to maintain compliance with statutory HR and employment requirements. Contractual and legal issues. • Increase demand • Inability to prepare adequately due to short notice from government. **Digital, Data and Technology** • Increased cyber-attack surface. • Data protection breaches. • Increased likelihood of audit findings or regulatory non-compliance during transition. • Insufficient business continuity and disaster recovery alignment across merged organisations.

	• Loss of public trust following service disruption, cyber incidents or data mishandling. • Reputational damage. • Skills gaps or loss of key ICT, cyber and data staff. • Supplier and contract risks. • Increased vulnerability and operational risk. • Failure to align cyber and digital strategies with the new authority's corporate objectives. • Delays to critical digital transformation. **Communication and Engagement** • Reduced morale leading to decreased performance or increased sickness and staff turnover • Damage public and staff trust and confidence in the new unitary council and arrangements • Relationships strained and weakened within the organisation and wider council collaboration, at all levels • Perceived loss of local identity. • Increased anxiety and frustration for staff • Misinformation filling gaps • Loss of trust in current council, new councils and decision-makers (both internally and externally) • Increased challenges from communities, MPs or the media • Damage to long-term trust, reputation and credibility • Confusion causing increased pressure on customer services **Financial** • Greater financial cost to NSDC. • Increase on budget demand pre section 24. • Cost pressures or unplanned expenditure falling to NSDC. • Failure to deliver of capital programme from the community plan (see SR605) **Operational delivery (BAU)** • Disruption to critical services during the transition period, particularly customer-facing or statutory services. • Reduction in levels of customer service/deliver leading to customer dissatisfaction. • Failure to deliver existing priorities (diverted resources due to LGR). • Reputational damage. • Loss of identity to NSDC & equity of service across all service user groups. **Governance and Shadow Authority** • Conflict pressures of having dual hatted members, which potentially impacts their capacity, availability, focus, or effectiveness in LGR. • Governance arrangements not established on time or operating ineffectively. • Unclear accountability delayed or poor decisions, or inadequate oversight during LGR transition. • Loss of local control.

	• Ineffective/delayed decision making from shadow authority/ programme directors impacting smooth transition and business as usual (finances, staff etc.) • Increased level of frustration amongst members due to loss of local control. • Post shadow elections, create space for senior leaders to shape the council's future and integrate new leaders into programme governance early.