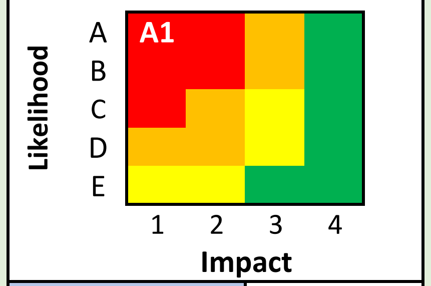
# City Security

## Description

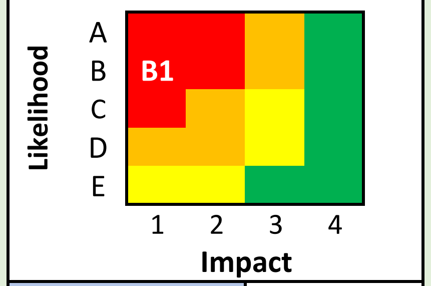
Major security-related incident in 'crowded places' as a result of international or domestic terrorism.

## Inherent Risk



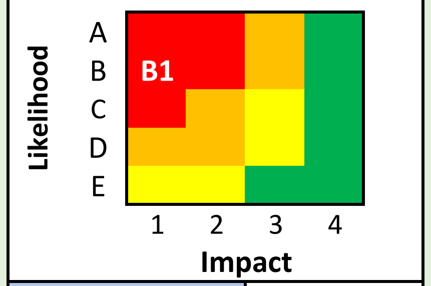
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q2 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | N/A |

## Risk Owner(s)

**Chris Lee**
(Gavin Macho)

**Andrew Gregory**

**Councillor Huw Thomas**
Leader

## Potential Impact(s)

**Immediate / Short-Term**

- Large numbers of fatalities, injuries to public
- Extensive structural damage and/or collapse of buildings
- Closure of roads having impact on transport network and access to businesses and properties.
- Damage/disruption to utilities (gas, electricity, water etc.)
- Immediate impact to core business, retail and sporting district in the centre of Cardiff

**Ongoing / Longer Term**

- Reputational risk due to a public perception Cardiff is an unsafe place
- Area viewed as a risk for potential future business investment.
- Inability to attract major future national and international events (political, sporting etc.)
- Increase in demand for Council services/support for all affected.
- Current economic climate to reduce the effectiveness of any recovery/regeneration of the area.

## What we've done/are currently doing to achieve the Residual Risk Rating

- All existing identified high-risk, crowded places have been formally assessed

- Some crowded places have an extremely limited and in some cases 'third party managed' access control process to operate them; providing little/no challenge

- CONTEST Protect/Prepare Task & Finish Group maintains the City Gateways Public Realm Enhancement Scheme, with agreed options for suitable PAS 68/69 mitigation for appropriate boundary locations; referred to as 'gateways'

- The work done in the city to address security concerns has been predominantly focused on the provision of physical assets to mitigate against the threat of hostile vehicles

- Areas protected against the threat of hostile vehicles include the Principality Stadium, St Mary Street, Queen Street, St David's Dewi Sant and Cardiff Bay.

- The Cardiff City Centre Access Control Protocol is currently operating at the heightened response level, reflecting the UK National Threat Level; permitting vehicles onto the pedestrianised areas within Cardiff City Centre using strict parameters

- Cardiff has led the way in Wales in relation to adopting comprehensive security measures for its City centre. This has been recognised in the development of new Welsh national structures, the Protective Security Preparedness Group (PSPG), which follows our historic Protect Group.

- The Cardiff PSPG is chaired by the Chief Executive and meets every 3 months. It has commissioned a major strategic review of all City Centre Security matters with reference to how existing arrangements will fit into the new developments coming online. A draft of the Cardiff Infrastructure Report, how we currently manage security infrastructure in the city centre, has been put together. Next steps include incorporating recommendations/ prioritising interventions, as well as seeking input and feedback from key stakeholders. Further discussions will be necessary regarding the report and its findings. It is hoped that a summary of the report and its findings will be presented at the next PSPG meeting in January 2022.

- The development of the PSPG has constituted in a CONTEST Board review which with new governance is providing security a growing focus.

## What we plan to do to meet target

- The PSPG Chair has commissioned a Director led review across all relevant Service areas to assess current operational and tactical arrangements for City Security to see if they are effective. All opportunities for improvement to captured and costed.

- The PSPG is broadening its remit by taking on a more comprehensive portfolio of security issues inclusive of Cyber Security ,Insider threat and personal security. Training and development being planned, projects managed at director level.

- Consideration to be given to incorporating structured and strategic conversations about security and counter terrorism into pre application stage of major developments.

- The PSPG will try to engage with Government to find funding to improve and develop Cardiff's security arrangement. Shovel ready projects ready to go.

- The Cardiff PSPG to reach out to Swansea and Newport so the 3 cities can support each other in the development of best practice.

## Type(s) of Impact

| | |
|---|---|
| • Service Delivery | • Health & Safety |
| • Reputational | • Partnership |
| • Legal | • Community & Environment |
| • Financial | • Stakeholder |

## Linked Risks

## Key Indicators / Measures used to monitor the risk

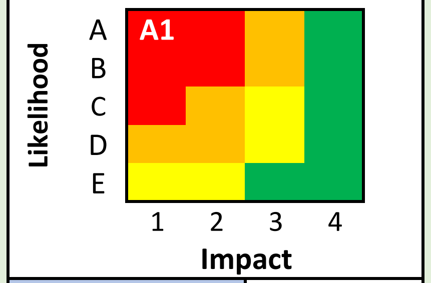
- National Threat Level and period at level
- No of 'Crowded Places' not protected to PAS 68/69 level

# Budget Monitoring (Control)

## Description

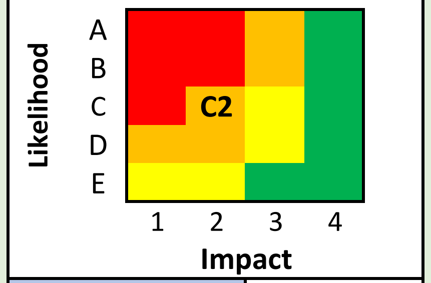
Failure to achieve the budget set, inclusive of budgeted spend and savings across Directorates, with increased use of emergency finance measures and the unplanned drawdown of reserves.

## Inherent Risk



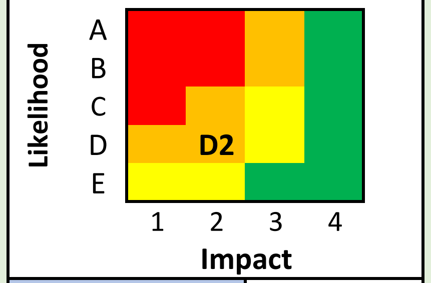
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q2 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | Q4 2021/22 |

## Risk Owner(s)

| | |
|---|---|
| **Chris Lee**<br>(Ian Allwood) | **Councillor**<br>**Chris Weaver**<br>Finance, Modernisation and Performance |

## Potential Impact(s)

- Inability to balance spend against budget, for the financial year

- Requirement to implement emergency measures to reduce spending during the financial year thus adversely impacting on ability to meet Corporate Plan objectives

- Requirement to draw down from General Reserves at the year end

## What we've done/are currently doing to achieve the Residual Risk Rating

- Clear financial procedure rules that reduce the level of risk of financial commitments being identified late in the financial year. The rules clearly set out the roles and responsibilities for budget management and are an area of interest for internal audit
- The first six months has seen monthly WG Hardship claims for additional expenditure and the first quarter of lost income. Continued due diligence is in place to ensure that all claims are solely related to the pandemic and follow the terms and conditions of the claims process. Review of assumptions of the rate in which services will return to budgeted levels over the financial year and align it with assumptions on WG Hardship grant. These controls plus regular review with impacted service areas and a sign off process is in place to mitigate against the risk of any payback requirement at a future point.
- Loss of income claims are also reviewed to ensure they reflect the reality of the time claimed and where applicable adjustments to pay back are made in a timely fashion. The forecast for the latter six months is less uncertain as the year progresses but there remains a level of uncertainty due to incidence of the pandemic, financial and the economic climate.
- The Corporate Director of Resources, Chief Executive and Cabinet Members have held two challenge meetings in the first six months of 2021/22 in order to ensure there is a focus on understanding any impending financial matters and any mitigations needed to be put in place in order to improve / maintain the respective Directorate financial position where appropriate.
- Continued monitoring of exceptional price fluctuations in respect to Building, transport, energy and infrastructure materials in order to forecast the extent and duration of these pressures. Close working with Service areas in order to identify cost pressures and compensating mitigation strategies that impact on delivery of Capital Programme and repair schedules to ensure works remain within budget.
- Risk assessment process put in place for 2022/23 Capital Programme which will identify obstacles to cost and timescale thus encourage early mitigations.

## What we plan to do to meet target

**2021/22 and the Medium Term**

- Develop with directorates the risk assessments and mitigations for each area of capital spend.
- Continue an appropriate level of due diligence in respect to Hardship Grant Claims in order to reduce the risk of significant under / over claiming
- In Early Q3, all Directorate Risk Registers will be reviewed in order to ensure the key financial risks are captured and mitigations are in place.

## Type(s) of Impact

| | |
|---|---|
| • Service Delivery<br>• Reputational<br>• Legal<br>• Financial | • Stakeholder |

## Linked Risks

Financial Resilience

## Key Indicators / Measures used to monitor the risk

- Monthly Directorate Monitoring reports detailing likely outturn position and performance against savings accepted
- Review of use of earmarked reserves and balances - Half Yearly
- Amount of Hardship Support claimed successfully

# Financial Resilience

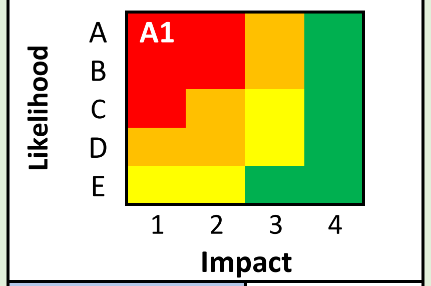
## Description

- Failure to deliver a balanced annual budget and a fully informed Medium Term Financial Plan.

- Lack of appropriate mechanisms to identify and manage unexpected financial liabilities.

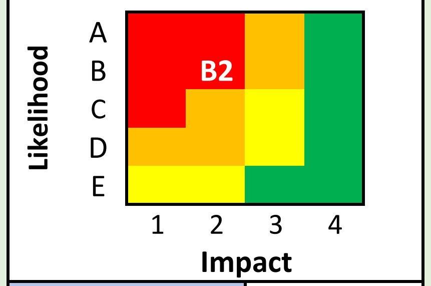
- The current outlook is that there is a Budget Gap of £81 million for the period 2022/23 to 2025/26.

## Inherent Risk



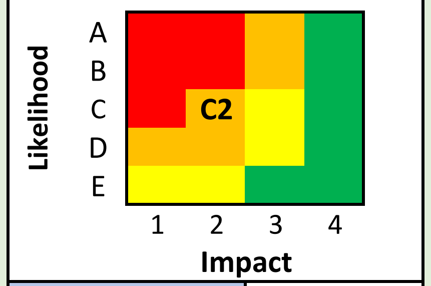
|  |  |
|---|---|
| **Last Reviewed** | **Q2 2021/22** |
| **Last Revision** | **Q2 2021/22** |

## Residual (Current) Risk



|  |  |
|---|---|
| **Movement from prev Qtr** | ↔ |

## Target Risk



|  |  |
|---|---|
| **Target Reduction Date** | **Q4 2021/22** |

## Risk Owner(s)

| | |
|---|---|
| **Chris Lee**<br>(Ian Allwood) | **Councillor**<br>**Chris Weaver**<br>Finance, Modernisation and Performance |

## Potential Impact(s)

- Failing to meet statutory obligations and potential for service delivery to be adversely affected.
- Reaching the point where a s114 notice is required to be issued by the S151 Officer.
- Reputational damage to the Council.
- Needing to draw down significant unplanned amounts from reserves.
- Levels of borrowing become unsustainable.
- Inability to progress policy initiatives.
- Inability to manage adverse external factors - e.g. adverse settlements, WG rent policy etc.
- Financial constraints and budget proposals result in unintended consequences such as increased instances of non-compliance and financial impropriety.
- Requirement for significant savings at short notice that are therefore not identified in a coherent, strategic way and which impact on service delivery.
- Level of borrowing limits the ability of future generations to take forward new priorities.

## Type(s) of Impact

| | |
|---|---|
| • Service Delivery<br>• Reputational<br>• Legal<br>• Financial | • Stakeholder |

## What we've done/are currently doing to achieve the Residual Risk Rating

**2021/22 and Medium Term**

- Regular monitoring to understand the in-year position and gain early insight into emerging risks that need to be factored into the MTFP work.
- Engaging and working in partnership with directorates during the budget process to ensure that budget proposals and services are deliverable within timescales and quantum (revenue and capital)
- Mechanisms in place such as Treasury Management Reserve and Financial Resilience Mechanism in order to dampen the impact of a worse than anticipated financial climate / settlements.
- Preparation of Prudential Indicators and a local affordability indicator to help assess the affordability, prudence and sustainability of the capital programme and associated levels of borrowing
- Close alignment with Corporate Plan objectives, to ensure resources are allocated appropriately, and that longer term financial savings are developed in enough time to be realised.
- Regular review of contingent assets and liabilities, and provisions to ensure the Council has adequate cover for emerging liabilities.
- Robust monitoring of the impact of C19 to ensure all eligible items have been claimed in- year.
- An approved TM Strategy to mitigate risk - incorporates borrowing at fixed rates to reduce exposure to future interest rate fluctuations
- A Major Projects accountancy function supporting the identification of key risks / financial issues in relation to large schemes.
- Maintaining approach to robust financial control mechanisms and strengthening complex / areas of risk through training e.g. VAT.
- Undertaken intial assessment against CIPFA FM code with high level findings
- Work on establishing the financial implications to services both in the short, medium and long term because of the impact of the Covid 19 crisis, and detailed log of budgetary issues affecting 2022/23.

## Linked Risks

Budget Monitoring (Control)

## What we plan to do to meet target

**2021/22 and the Medium Term**

- Autumn CEXEC Budget Challenge Sessions focussing on modelling work, COVID impact, 2022/23 savings work to date.
- Consider and take any opportunities to increase earmarked reserves in order to provide first line of defence against financial shocks.
- Review corporate approach to business case development, approval and post project monitoring to ensure expenditure assumed to pay for itself can do so over its expected life.
- Strengthening links between financial planning and asset management strategies, which consider the current condition of assets and future requirements.
- Identify clear, detailed plans and timescale for delivery of capital receipts targets.
- Enhance focus on a multi-year position (recognising limitations where settlement information is for one year only.)
- Review approach to governance and financial monitoring of special purpose vehicles to ensure liabilities and any financial guarantees are understood and are appropriate.
- Complete self-assessment against the CIPFA FM code and Balance Sheet Review and develop implementation plan in respect of any findings or recommendations, which provide further financial resilience.
- Confirm approach and reporting of commercial investments as part of standard monitoring processes and reports.
- Continue to keep cost pressures arising from BREXIT, supply chains issues and labour / skills  shortages under review in terms of their impact on costs, inflation and interest rates and the impact of these for the MTFP and Capital Programme

## Key Indicators / Measures used to monitor the risk

- Financial Snapshot which highlights historical & current performance with regards budget monitoring, achievability of savings, levels of borrowing, and financial ratios.
- Outturn vs Budget: Main budget lines under or overspend as a % of budgeted expenditure.
- Delivery of planned savings: Total (£) unachieved planned savings as a % of total (£) planned savings.
- Use of reserves: 1) Ratio of useable reserves to Net Revenue Budget (NRB), 2) Amount of useable reserves used to balance budget as % of NRB.
- Council tax: 1) Council tax and other income as % of NRB, 2) Council tax collection rates (in-year actual).
- Borrowing: 1) Total commercial investment income as % of total net general fund budget, 2) Total (£) commercial investments and (£ plus%) amount funded from borrowing, 3) Borrowing related to commercial investments as % of General Fund total borrowing, 4) Capital interest costs and MRP as a proportion of NRB.
- Performance against Budget Timetable.
- Frequency / timeliness of engagement with SMT/Cabinet.
- Proportion of Savings Proposals in Realised or at Delivering stage.
- Section 151 Officer Statement in respect of capital strategy, adequacy of reserves and other statutory commentary.

# Fraud, Bribery & Corruption

## Description

Fraud, financial impropriety or improper business practices increase as internal controls are weakened as resources become severely stretched.

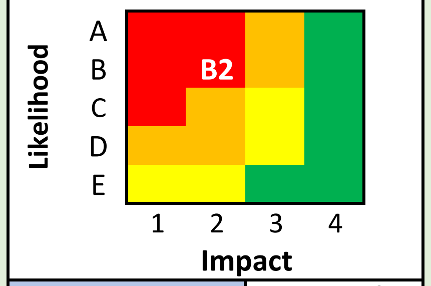
## Potential Impact(s)

- Increase in frauds and losses to the Council
- Reputational risk as more frauds are reported
- Increased time investigating suspected fraud cases impacting on capacity

## Type(s) of Impact

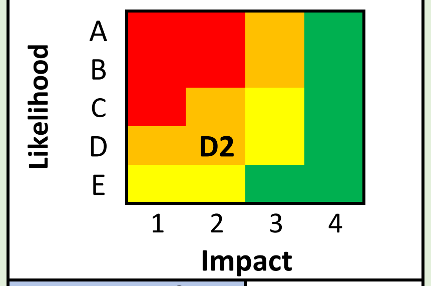
| | |
|---|---|
| • Service Delivery<br>• Reputational<br>• Legal<br>• Financial | • Stakeholder |

## Inherent Risk



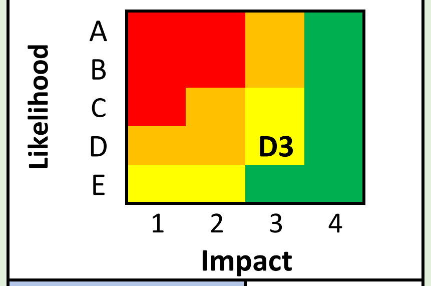
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q1 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | 2022/23 |

## What we've done/are currently doing to achieve the Residual Risk Rating

- The Council communicates a zero tolerance approach to fraud, bribery and corruption.
- Regular review of relevant policies and procedures e.g. the Fraud, Bribery and Corruption Policy, Anti-Money Laundering Policy and Disciplinary Policy.
- Financial Procedure Rules and Contract Standing Orders and Procurement Rules and training.
- National Fraud Initiative data matching exercises in collaboration with the Cabinet Office and Audit Wales.
- Receipt and dissemination of fraud intelligence alerts from law enforcement agencies.
- Regular reports to the Section 151 Officer, Governance and Audit Committee, Portfolio Cabinet Member and the Chief Executive.
- Governance and Audit Committee review of the risk management, internal control and corporate governance arrangements of the authority.
- Independent assurance from Internal and External Audit on the effectiveness of governance, risk and control.
- Briefings developed and disseminated to Schools on fraud and control risks.
- Provision of disciplinary management information on DigiGOV.
- Mandatory disciplinary e-learning module for all managers to complete and a programme of mandatory e-learning modules and training for Disciplinary Hearing Chairs, Investigating Officers and Presenting Officers.
- Fraud Publicity Strategy, to publicise the Council’s approach to counter fraud work / sanction activity and explain the roles and responsibilities of key parties.
- Counter-Fraud and Corruption Strategy approved by Cabinet in July 2019, with associated Fraud Awareness eLearning rolled out to all pc users commencing.
- Face-to-Face Fraud Awareness training delivered to officers and headteachers in quarter 3 and school governors in quarter 4 2019/20.
- Participation in International Fraud Awareness week commenced in November 2019, undertaken annually thereafter.
- Investigation Team participation in SMAS triangulation exercise, commenced in quarter 3 2019/20.
- Investigation Team provision of investigation and counter-fraud advice, guidance and support to Directorates as required.
- SMT participation in fraud tracker and assessment commenced January 2020, with commitment to full exercise at least annually.
- Revised 'Anti-Money Laundering Policy' approved by Cabinet in Q3 2020/21 and eLearning rolled out to officers with key roles and those working in high-risk areas.
- ‘Authorisation and Protocol Requirements for Review of Work Activities’ approved by Cabinet in Q4 2020/21.

## Linked Risks

## Risk Owner(s)

| | |
|---|---|
| **Chris Lee**<br>(Ian Allwood) | **Councillor**<br>**Chris Weaver**<br>Finance, Modernisation and Performance |

## What we plan to do to meet target

- Consultation of an Internet Investigation Procedure.

- Review the suite of Counter-Fraud Operational Policies alongside the review of the Council’s Disciplinary Policy commencing 2021/22.

- Monitoring and reporting completion rates of mandatory fraud awareness training and anti-money laundering training.

## Key Indicators / Measures used to monitor the risk

- Mandatory Fraud Awareness eLearning completion and face-to-face attendance rates
- Anti-Money Laundering eLearning completion rates
- Delivery of Fraud Awareness week campaign annually
- Delivery of Policy updates in accordance with associated targets
- Delivery of mandatory investigating officer training and the note taker training
- Timely completion of casework and investigations
- Provision of timely investigation and counter-fraud advice, guidance and support to Directorates
- Adherence to the NFI Security Policy and annual completion of compliance forms

# Information Governance

## Description

Information handled inappropriately leaves the Council exposed to intervention and financial penalties issued by the Information Commissioner (ICO). This includes information held by Cardiff Schools.

## Potential Impact(s)

Leads to the Information Commissioner issuing notices of non-compliance

These could consist of:

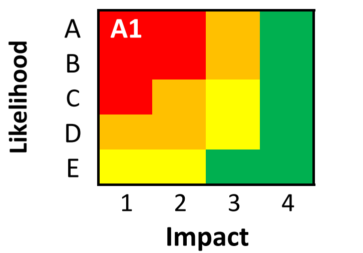
• A "Stop Now" Order which would mean that no personal data could be processes by the Council in its entirety
• An Information Notice which would mean that a service would have to provide information in a very limited period thereby impacting on service delivery
• A Decision Notice could be issued as a result of non compliance with an FOI/EIR request which would require information disclosure
• Undertaking which requires an Action Plan of Remedial Measures which would be subject to ICO Audit
• Enforcement Notice requires immediate improvement action to be put in place
• Financial Penalty up to £17.5 million for Higher Level Tier and £8 million for Lower Level Tier breaches of the Data Protection Act.
• Compensation unlimited liability claims for damages as a result of a data breach from individuals.

## Type(s) of Impact

• Service Delivery
• Reputational
• Legal
• Financial

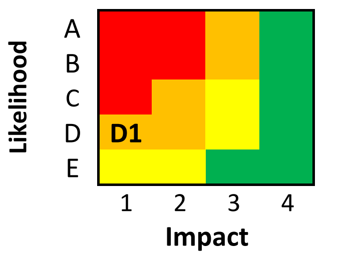
• Stakeholder

## Inherent Risk



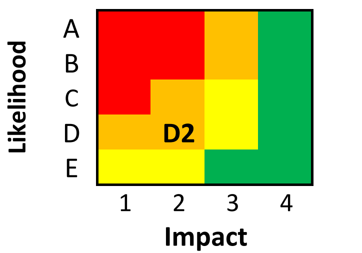
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q2 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | Q4 2021/22 |

## Risk Owner(s)

**Chris Lee**
(Dean Thomas)

**Councillor**
**Chris Weaver**
Finance, Modernisation and Performance

## What we've done/are currently doing to achieve the Residual Risk Rating

• Suite of Information Governance Processes, Policies and Strategies in place and annually updated for 2021.
• Gold level assurance has been achieved through the annual Cyber Security Plus ISAME Accreditation in September 2021, the next annual accrediation of this process will take place in September 2022.
• An established Information Governance & Security Board meets quarterly. A quarterly Information Governance Report and briefings of decisions or recommendations for Board are provided on a quarterly basis.
• Processes are established through procurement and ICT for ensuring Data Protection Impact Assessments are completed if personal data is being processed
• A corporate Information Asset Register is held which details personal data assets held by each Council directorate. This is annually reviewed with the next review scheduled for August 2022.
• Service Level Agreements in place where Cardiff Council is the Data Controller for regional services, including Rent Smart Wales, National Adoption Service and Cardiff Capital City Deal
• Advice, guidance and support is provided to all Cardiff Schools through Service Level Agreements.
• Corporate Retention schedule in place and updated annually in line with any legislative changes.
• Information Governance Maturity Model established to monitor risks against areas of information governance to feed into corporate risk status.
• The Digitalisation of Paper Records Strategy and associated business process changes are in place with alternative delivery contracts in place to support increased paper storage demands, with processes established to support corporate programmes.
• Data Protection e-learning training available for Council staff to complete before 31 December 2021. Managers are able to monitor compliance with information provided as part of the Information Governance Board Report.
• National and Regional Information Governance Agreements in place in respect of covid-19 data processes, including Cardiff & Vale TTP Information Governance agreements and National Joint Data Controller Agreements
• An updated data processor agreement, representing changes to UK laws post Brexit in place to support data processor arrangements and the Council's standard contract terms and conditions
• An Information Governance Champions Group has been established. The Group of IG Champions will be responsible for monitoring and reporting IG compliance into the Information Governance & Security Board
• Processes have been established to enable Information Governance & Security Board to have oversight of DPIA's completed against Procurement Contract Awards where personal data is processed •
A new streamlined surveillance system DPIA process is established to ensure services manage privacy responsibilities and link into corporate infrastructure solutions

## Linked Risks

## What we plan to do to meet target

• Support Information Governance Champions with a review of their directorates Information Asset Registers to ensure that these are accurate and up to date. Q3
• Information Governance continue to support Legal Services and HR with ensuring that an appropriate agreement is put in place to manage data protection risks associated with employee information data transfers and handling with TCS. Q3
• Monitor compliance with e-learning training in line with the revised target date for completion and work with the academy to create new content for 2022. Targeted support will be provided to Social Services during Q3 2021/22 to improve compliance within these high level risk areas. Q3
• Work with Childrens Services and implement new service delivery model for management of social services requests. This will improve compliance, accountability and processes for managing social service disclosures. Q3 •
Continue to monitor directorate risk registers for information governance risks and reporting any concerns to Governance & Security Board. Q3
• Continue to work with Schools to develop DPIA's on MyConcern and Skodel with support with relevant school. Q3 •
Establish processes and reporting of data protection breach claims. Q3
• A project brief outline to be provided in respect of alternative service delivery models for the Council's Records Centre, linked to the Atlantic Wharf Regeneration, Core Offices and Recovery and Renewal Programmes. Q3
• Conduct a review of the Council's Publication Scheme requirements through the Information Governance & Security Board. Q3
• Review with the Head of Assurance how business data, not personal data, risks are managed and link into IG corporate processes, and determine who owns corporate risks for business data Q3
• Release training and education communications to support schools with their Information Governance responsibilities •
Develop an Information Governance awareness week to link into national data protection day and FOI day. Q4

## Key Indicators / Measures used to monitor the risk

• Suite of IG Indicators/Service Metrics
• No. of ICO complaints
• No. of FOI /EIR SAR Requests
• No. of individuals trained on Data Protection
• No of Data Protection Impact Assessments being undertaken
• No of data protection breach complaints/claims

# Cyber Security

## Description

There are 11 areas of potential risk within the National Cyber Security Centre cyber risk model. Of these, nine are assessed as well controlled within the Council

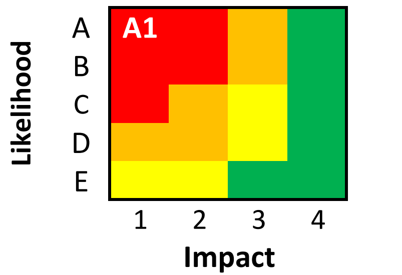
Three of the eleven areas of a Cyber Security assessment underpinning the corporate risk have been identified as high risk as follows:

**Monitoring** - the volumes of systems, applications and audit logs do not lend themselves to easily assess how and when systems are being used, leading to an ineffective response to deliberate attacks or accidental user activity

**Secure Configuration** - Increased risk from malware and ransomware.

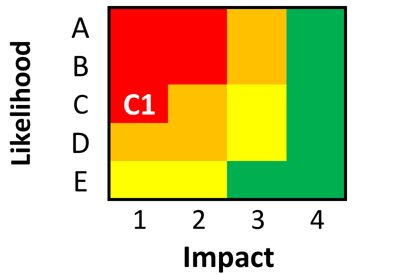
**Corporate Cloud Security** - 2018 Internal Audit identified contract, SLA and service management weaknesses in externally hosted services

## Inherent Risk



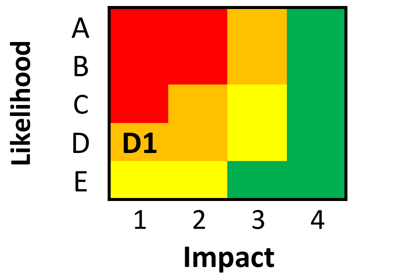
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q1 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | 2022/23 |

## Risk Owner(s)

| | |
|---|---|
| **Chris Lee**<br>(Phil Bear) | **Councillor**<br>**Chris Weaver**<br>Finance, Modernisation and Performance |

## Potential Impact(s)

The intent of cyber attackers includes, but is not limited to:

- financial fraud;
- information theft or misuse,
- activist causes to render computer systems intolerable and to disrupt critical infrastructure and vital services.

The impact of a cyber-attack / incident has the potential to involve the realisation of the risks associated with:

- An information governance breach (i.e. Stop Now Order, Information Notice, Enforcement Notice, Financial Penalty etc.)
- A business continuity incident – with a potential for major loss of service and legal, health and safety and financial implications.
- A financial / fraud related attack.

A malicious attack could result in loss of confidence from those transacting with the Council (reputation), as well as legal, asset, system, operational and financial implications.

## What we've done/are currently doing to achieve the Residual Risk Rating

The principal controls for the high risk areas are as follows:

**Monitoring**

- Log analysis is undertaken on a prioritised basis with incident reporting to ISB and discussed with IAO - risk of vulnerabilities could be further mitigated with additional resourcing for log monitoring - this is under continual review

**Secure Configuration**

- Corporate - Procurement of replacement devices and outdated applications
- Above will facilitate management review of cost of replacement and enable greater planning of replacements.
- ICT: Early and clear notification to service and systems owners of when solution will need replacing or upgrading.
- ICT: Tougher stance on removing or blocking systems and services that are not fully supported by suppliers and as such may pose a risk to security and compliance.
- ICT Malware / Ransomware Risk Report has been submitted for review by ICT Management.

**Corporate Cloud Security**

- Maturing PIA & CIA process used to assess risks to data and technology solutions

- Independent assessment and certification of the council's IT security posture via the National Cyber Security Centre (NCSC) Cyber Essentials Plus scheme
- Independent assessment and certification of the Council's Information Governance (GDPR/Data Protection) posture via the ISAME Governance scheme, awarded at the highest level of Gold
- Staff Cyber Security training programme rolled out to all staff to give guidance on threats and how to spot

## What we plan to do to meet target

- ICT and Information Governance (IG) Teams to continue to liaise with FM for physical security assurances and to promote an incident reporting culture.

- To ensure strong ICT security, monitoring and cloud security controls:

- ICT lifecycle and notification targets are being monitored and managed through the 'ICT Platforms' risk actions
- Collaboration between ICT and IG to develop and map current ICT system providers in phased development of an Information Asset Register
- Privacy Impact Assessment / Cloud Impact Assessments to be reviewed to ensure compliance with the requirements of the General Data Protection Regulation (GDPR) Action Plan being managed by the Information Governance Team
- Governance and management requirements to be formalised for periodic and systematic review of all ICT systems.

- SIRO to review / consider Cloud Infrastructure to ensure:

- Assurance of effective governance and management
- Resource, risk appetite and outcomes required
- Education of business systems owners in risk and management of cloud based services.

- ICT Management to review Malware report and implement improvement actions

## Type(s) of Impact

| | |
|---|---|
| • Service Delivery<br>• Reputational<br>• Legal<br>• Financial | • Health & Safety<br>• Stakeholder |

## Linked Risks

Information Governance

## Key Indicators / Measures used to monitor the risk

- Threat intelligence from National Cyber Security Centre (NCSC), including national posture and guidance via the National Cyber Security Strategy/Programme
- Threats and risks highlighted by NCSC Cyber Security Information Sharing Partnership (CiSP), Cymru WARP (Warning, Advice and Reporting Point) and Welsh Government/WLGA
- General UK posture and issues raised in national and local media
- Number of compromises - breaches are monitored, investigated and reported back via Information Security Board and where applicable the ICO
- Monthly reporting of number of virus attacks via email blocked

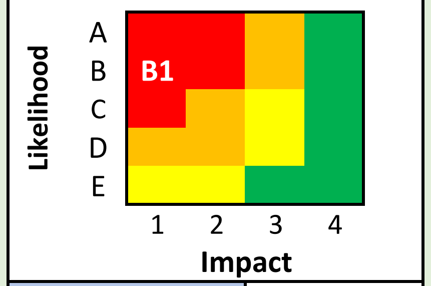
# Business Continuity

## Description

Large scale incident/loss affecting the delivery of services.

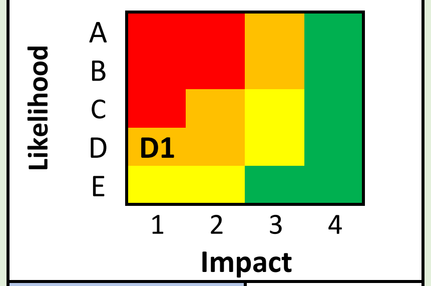
The potential risk is that our most time sensitive activities are not sufficiently resilient and fail, following an incident which impacts on their delivery and that our incident management structure, used in response to internal incidents and external emergencies, also fails in response to an incident.

## Inherent Risk



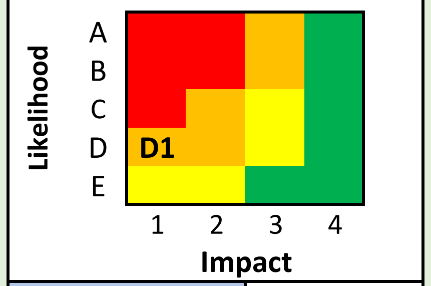
| | |
|---|---|
| Last Reviewed | Q2 2021/22 |
| Last Revision | Q2 2021/22 |

## Residual (Current) Risk



| | |
|---|---|
| Movement from prev Qtr | ↔ |

## Target Risk



| | |
|---|---|
| Target Reduction Date | N/A |

## Risk Owner(s)

| | |
|---|---|
| **Chris Lee** | **Councillor Huw Thomas**<br>Leader |

## Potential Impact(s)

- **Health and Safety** – potential impact on staff and on the public relying on our most, time sensitive, critical services

- **Legal action** -Failure of key services could lead to Legal action against the council

- **Financial** - Failure of key services could led to significant financial cost both in terms of Ombudsman action and Enforcement action from regulatory bodies, as well as individual legal action against the corporate body where service failure leads to legal action against us from private claimants

- **Reputational** - Impact on key services to the public could lead to significant reputational damage to the organisation

- **Stakeholder** – Impact on key stakeholders as result of failure

- **Service delivery** – Potential significant impact on service delivery to the public, impact of key services could lead to significant impacts to the public and the corporate body un delivering its services

## What we've done/are currently doing to achieve the Residual Risk Rating

- The Council has a BCM Champion who sponsors BCM at a strategic level
- We have an approved Business Continuity Policy which is aligned to ISO22301
- BCM toolkit is now available on CIS
- The Council employs a Business Continuity Officer who is a qualified ISO22301 lead auditor
- The Emergency Management Unit has developed an Incident Management Plan (Cardiff Council's Emergency Management Plan) to ensure alignment with ISO22301. This was fully updated in March 2019.
- The Council has a 24 hour Incident Management structure for Gold and Silver Officers.
- Cardiff Council is a member of the Core Cities Business Continuity Group
- Internal Audit completed an audit of the Business Continuity Risk in September 2018 and the assurance statement was "Effective with opportunity for improvement"
- Q4 of 2019/2020 saw the council undertake a full review and update of the activities delivered across the council allowing us to focus on the resilient delivery of key functions as we planned and responded to the COVID19 threat. This review was delivered at the Strategic Level.
- Each Directorate was tasked with reviewing and updating their key business continuity plans in preparation for the emerging COVID19 threat. Each Director/Corporate Director was responsible for ensuring this work was undertaken fully and properly. The existing Business Continuity work provided a solid foundation to our response to the COVID19 threat.
- The full corporate incident management team was activated in early March.
- The Council worked positively at a Local Resilience Forum(LRF) level with partners supporting a wider Wales response to the COVID19 threat. This included daily reporting and escalation of key issues to the LRF.
- Areas were forced to change to a far more agile way of operating with our core ICT requirements changing to support far more agile/home working. The mode of delivery worked exceptionally well and provides the potential for longer-term resilient agile working in response to the ongoing COVID19 risk, in addition to positively supporting other aims and corporate risks.
- Staff across the council adapted at speed and have worked incredibly hard to deliver key services in new ways, in addition many staff changed roles to support the resilient delivery of key services and new asks on the council to keep the public safe.

## What we plan to do to meet target

- Work with ICT to ensure our core infrastructure is as resilient as possible and able to support additional agile working capacity.
- Work with the teams involved with looking at the potential of using alternative delivery models for council services. Identifying risks associated with alternative delivery models for specific services and recommend potential risk management solutions for implementation, to protect the delivery of our most critical services.
- The BC Officer is working to develop and enhance individual Directorate response capability to ensure Directorates are in a stronger position to respond to incidents which could impact on the Council and our most time sensitive activities
- The BC officer is continuing a review of 4x4 resources across the council to support our response capability to deal with the potential of winter storms.
- The BC officer along with the Resilience Unit are continuing to ensure that corporately we are able to respond to the COVID19 threat and the ongoing risk including of a third wave until the threat of the pandemic has fully dissipated.
- The Resilince Unit will undertake a lessons learned review of key lessons from the first 2 waves of the pandemic and ensure that key risks/lessons/processes that feed into the councils resilience capability are incorporated into our ongoing planning to support us in being ready for ongoing risks. This will, where appropriate, involve a review and update of individual BC plans by Directorates and also a review and update of the councils Emergency Management Plan.
- The Resilience Unit will support Directorates in their Autumn/Winter 2021 resilience planning with targeted work and support around the councils most time critical activities. As the challenges the pandemic continues to pose for the council along with the other current and emerging risks this work will focus on a continual and sustainable delivery of key services.

## Type(s) of Impact

- Service Delivery
- Reputational
- Legal
- Financial
- Health & Safety
- Stakeholder

## Linked Risks

Brexit Risk

## Key Indicators / Measures used to monitor the risk

The Red activity BC plan status is reviewed on a quarterly basis via a report to SMT after the CRR submission. Additionally the risk is managed as part of the Corporate Risk Management process via the CRR returns and the BC risk is also audited by Internal Audit . The last Internal Audit of the Business Continuity Risk was in in 2018.