Archwilydd Cyffredinol Cymru
Auditor General for Wales

WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Bridgend County Borough Council – Digital Risk Diagnostic

Date: November 2018

Author: Andrew Strong

Digital Risk Diagnostic - Scope

- Wales Audit Office review for planning purposes
- To identify and understand the key digital risks the Council faces
- Fieldwork completed May & June 2018
- Document review July 2018
- We thought we would share the key findings and messages with you for discussion

Key areas and risks

Key areas	Risk
1. Digital Strategy and Transformation	Missed opportunities and delayed implementation of digital projects to support the MTFS.
2. Website development - being better connected	Does not fully support ‘channel shift’ and expectations of service users.
3. Resilience of the ICT infrastructure and platforms	Does not support the new digital and transformation projects.
4. IT skills, capacity, capability and resources	Threat to the timely delivery of digital change projects and to standards required.
5. ICT Disaster Recovery (DR) planning	Delays in recovering from IT service interruptions.
6. Cyber security and resilience	Threat to the confidentiality, integrity and availability of IT services and data.
7. Data protection arrangements & GDPR	Risks from potential penalties if arrangements are not fully complaint.

1. Digital Strategy and Transformation

- Digital is a key enabler for transformation.
- Digital vision, roadmap and strategy being established for the transformation programme to modernise services and deliver efficiencies.
- MS Cloud Navigator process – workshops for channel shift, digital first and consulting service areas. Digital strategy development and agreement by end of 2018?
- Should be supported by adequate Transformation Programme governance and scrutiny. Risks include funded investments plans, delivery plans and realising benefits.
- Information Management strategy requires updating.

2. Website

- SOCITM 2016 1* Better Connected rating – a basic score.
- New website April 2018 and ‘my account’ – phase 1 with a limited number of ‘transactions’ eg Council tax.
- Further developments required – phase 2 – reporting and transactions eg pot holes and school admissions.
- Phase 3 developments …… ?
- Risks to ‘channel shift’, digital project delivery, integration to back office functions & processes and to ‘mobilise’ the workforce.

3. Resilience of the ICT infrastructure and platforms

- Resilience and cyber risks from out-of-date and unsupported ICT infrastructure estate and platforms.
- Technology refresh plans to prioritise replacement of end-of-life ICT infrastructure are challenged by a lack funding available.
- The Council have recently invested in and implemented new Storage Area Network devices.
- Scope to consider data centre storage approach vs cloud based IT service models.
- Modern ICT infrastructure needed to support agile working & delivery of new digital transformation projects.

4. IT skills, capacity, capability and resources

- Risk that the ICT operating model is not adequate to deliver the Digital Strategy and Transformation.
- Is there the capacity, resources and digital leadership across the organisation to support the implementation of digital projects?
- Risk that the IT Department and Service does not have or cannot bring in the skills and knowledge to deliver the Digital Strategy on time.
- Is funding available from services for transformation?
- Scope to develop a wider range of IT key performance indicators that measure both IT service delivery, support and savings realised.

5. ICT Disaster Recovery (DR) planning and data backups

- IT DR plans require updating and further consideration for recent changes to ICT infrastructure and key system priorities.
- DR plans have not been fully tested to ensure they work as intended and to drive improvements in these plans.
- Risks to resilience planning should consider:
  - data centre approach and off-site data backup
  - potential for cloud solutions
  - backup approach and policy, do backups work?
  - assess impact on the Council of the Network Infrastructure Services (NIS) Directive.

6. Cyber security and resilience

- Council's Public Services Network (PSN) code of connection – fully certified?
- Addressing improvement action plans as a priority?
- IT security policy – update and review
- No cyber security risk assessment documented
- No regular scheduled internal network vulnerability assessments completed
- Scope to improve cyber incident response plans
- No gap analysis to Information Security Management standard (ISO 27001) good practice for assurance purposes and continual service improvements.

7. Data protection arrangements & GDPR

- GDPR readiness plans in place and appeared to be progressing in May 2018 (fieldwork date).
- Work still remained ongoing to reach full compliance and risks that this is likely to extend past the end of May 2018 implementation deadline. These include:
  - privacy notices, information asset registers and relevant policies being updated
  - training and awareness
  - retention schedules.
- Risk of impact on GDPR preparations on responding to FOIA and Data Protection statutory information requests.
- Corporate Director and SIRO has since left the Council after our review – succession plans in place ?

Next steps – consider risks

Key proposals for further consideration based on risks identified:

- Complete the Digital Strategy development, formally agree plans and provide adequate funding for the timely delivery of plans.
- Ensure the transformation programme governance and scrutiny arrangements are appropriate.
- Look at ways to develop the Council's website transactional and 'channel shift' capabilities.
- Complete GDPR compliance work and readiness plans and update the Council's information management strategy.
- Review the adequacy of the Council's IT infrastructure and network to support its emerging digital strategic approach.
- Consider reviewing the IT operating model to deliver the digital transformation strategy.

Next steps – consider risks

- Update and test IT Disaster Recovery plans and ensure these work as intended.
- Address potential cyber security risks by:
  - confirming the PSN code of connection certification
  - consider the cyber security risk assessment process and comparisons to ISO 27001 security management standard
  - complete internal network vulnerability risk assessments and cyber security incident response plans.