
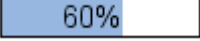
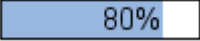
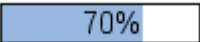
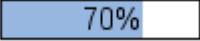



(02) Outstanding Audit Recommendations where Heads of Service have asked for an extension of time

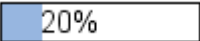
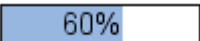
Code	Description	Progress Bar and Risk level	Latest Note	Due Date
20 BC 04 Testing of Service Resumption Plans	A test of each Service Resumption Plan should be undertaken at least on at least an annual basis. On completion of the test a lessons learnt report should be employed to update the plan. All such documentation should be retained in Resilience Direct.	 95% HIGH RISK	<p>Business Continuity Exercises' have been completed with managers and Heads of service for Place Property and Regeneration, Environmental Enhancement, Governance and Environmental Health and Housing. A Senior Management tabletop exercise is scheduled for Monday 5th June and a report will be submitted to SMT by the end of July. once this report has been signed off by SMT this action can be closed down as exercises will be ongoing on an annual basis.</p> <p>Further exercises that have been planned are with CCTV, Crematorium, Planning and PMO following this need being recognised during the service area exercise.</p> <p>Invites have been sent out to heads of service for 2024 exercises and a timetable of testing and exercising has been added to the exercise and testing strategy (attached).</p> <p>Request Revised due date: July 31st 2023</p>	01-Jan-2023


Code	Description	Progress Bar and Risk level	Latest Note	Due Date
20 MCS&BC 02 Implementation of Civica Financials Software V19.5, V20 & V21 should be report to the S&R in the quarterly performance report	The anticipated implementation dates for Civica Financials software releases v19.5 (interim), v20 and v21 should be recorded upon the Service Plan Actions section of the quarterly Performance and Financial Management report presented to the Strategy and Resources Committee.	 MEDIUM RISK	Testing of version 23.1 had largely been completed for a planned 31st March 2023 go live date. However, Civica Financials advised to delay go-live until version 24 had been released due to certain bug fixes. Version 24 will shortly go into our test environment so that we can test before going live. Time extension requested to 29th September 2023, in line with revised Service Plan target date.	31-Mar-2023
21 BCFU 01 Update the Implementation Management Plan	Observations: The Implementation Management Plan has not been updated since 2016. This is a core document which details the incident response structure, and involvement of senior managers. We recognise that there is a “standby manual” containing all current contact details, which has been tested through regular call exercises to ensure senior managers can be contacted. This helps mitigate the absence of a current Implementation Management Plan.	 HIGH RISK	Implementation plan V 1.1 was reviewed in May 2023 and will be validated at the SMT business continuity exercise on Monday 5th June, this action can be closed following the exercise report being issued in July. Request revised due date – July 31st 2023	01-Jan-2023

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
21 BCFU 05 Put appropriate focus on ICT	Given increasing reliance on home working and IT under the emergency, the Council needs to ensure significant focus is placed on ensuring there is sufficient resilience in this area. Specific issues include: • Pre 2016 several staff have removed from the ICT Team structure and there are several points of failure with some individuals who provide the sole support for specific areas / systems. Work is ongoing to train at least two members of staff for key systems. • The IT Disaster Recovery Plan, which was last updated in 2016. Further updates had been put on hold until there was clarity on the business priorities to inform recovery of their support systems etc. • Our recent audit on Cyber Security has recommended as a priority the need to understand the potential impact of a Ransomware attack on the Council, and the need to exercise the Incident Response Plan.	 HIGH RISK	<p>ICT have worked with our EP to identify NDCs critical systems to define our backup recovery architecture; these have been signed off by SMT. ICT have a PAG bid in place for our secondary data centre in Lynton House which will allow for for regular testing of our back-ups - this links with 21 CSM 17, 22 CS 11 and recommendations from our cyber treatment plan with DLUHC.</p> <p>Request revised date: 31st December 2023 to allow PAG to be approved, procurement, installation & testing.</p> <p>Other items under this recommendation; Staffing - we have a new structure in ICT which has given the Infrastructure Team an additional team member which will reduce the single points of failure. We will continue to ensure the team have the appropriate internal & external training as needed.</p>	30-Mar-2023


Code	Description	Progress Bar and Risk level	Latest Note	Due Date
21 BCFU 07 identify Key Contractor Services	<p>Observations: The Service Resumption Plans contain some analysis of the crucial contracted services which support delivery, albeit more detail could be provided. We suggest that the Council should consider what its top (five to ten) priority contracted services are, seek assurances from those suppliers that they have appropriate business continuity arrangements, and also what other alternatives might be put in place in the event of supplier failure.</p>	 70% HIGH RISK	<p>The identification of key contractor services for the first 1 month priority services has been completed (extended from 1 week previously identified). Assurance will be sought from the top 5 as a matter of urgency whilst work is underway to implement a standardised process for BC assurance moving forward (outside scope of this recommendation).</p> <p>Request revised due date– September 29th 2023</p>	01-Jan-2023
21 CSM&R 02 Remove internet & email access from privileged accounts. Provide administrators with an ordinary account for email & internet access.	<p>Remove internet & email access from privileged accounts. Provide administrators with an ordinary account for email & internet access.</p> <p>Observations and Implications Privileged user accounts (administrators) have internet access and mailboxes. Malicious code embedded or linked in web pages, email and attachments will execute with high privileges and wide system access.</p>	 90% HIGH RISK	<p>Rethinking the way the IT team does every task without IT admin access is one of the biggest culture changes we've introduced at North Devon Council. Historically ICT have been excellent at locking down end users whilst the ICT team have had access to everything.</p> <p>Privileged Access Management (PAM) is a critical element of our cyber security strategy. IT admin privileges have been de-scoped from 5 existing members of staff. Accounts for new members of the IT team are using the PAM system to access servers and administration consoles.</p>	31-Dec-2022

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
			<p>Further work needs to be done before the action can be closed. The Infrastructure Team are continuing to enhance the activities that can be done through PAM whilst ensuring they don't prohibit themselves from being able to do deliver their work as IT engineers.</p> <p>Request revised due date: 31st September 2023</p>	
<p>21 CSM&R 03 Follow NCSC guidance on applying the 'least privilege' model in authenticating for remote access.</p>	<p>Recommendation: Follow NCSC guidance on applying the 'least privilege' model in authenticating for remote access.</p> <p>Observations & Implications: Administrator Remote Access - Administrators authenticate for remote access with their privileged account. Attackers target vulnerabilities in remote access services and devices to obtain privileged credentials.</p>	<div data-bbox="860 890 1059 932" style="border: 1px solid black; background-color: #ADD8E6; padding: 2px; display: inline-block;">90%</div> <p>HIGH RISK</p>	<p>Rethinking the way the IT team does every task without IT admin access is one of the biggest culture changes we've introduced at North Devon Council. Historically ICT have been excellent at locking down end users whilst the ICT team have had access to everything.</p> <p>Privileged Access Management (PAM) is a critical element of our cyber security strategy. IT admin privileges have been de-scoped from 5 existing members of staff. Accounts for new members of the IT team are using the PAM system to access servers and administration consoles.</p> <p>Further work needs to be done before the action can be closed. The Infrastructure Team are continuing to enhance the activities that can be done through PAM whilst ensuring they don't prohibit themselves from being able to do deliver their work as IT engineers.</p> <p>Request revised due date: 31 September 2023</p>	<p>31-Dec-2022</p>

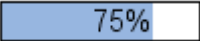
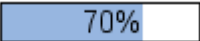
Code	Description	Progress Bar and Risk level	Latest Note	Due Date
21 CSM&R 17 Update recovery/restoration process to include specific steps to verify all systems used in the recovery are clean from malware/ransomware before connecting to the backup & starting recovery.	<p>RECOVER USING CLEAN DEVICES Recommendation: Update the recovery and restoration process to include specific steps to verify all systems used in the recovery are clean from malware and ransomware before connecting to the backup and starting recovery. Observation: Virtual server and desktop restore will be directly from the Arcserve backup. It is not clear how the Arcserve appliance itself, the VMWare ESXi host system and the client machines used to initiate the recovery are confirmed as malware-free. Implications: Restored systems may be re-infected with malware. Hypervisors may have been affected in the October 2020 Pysa ransomware and extortion attack on Hackney Council.</p>	 20% HIGH RISK	<p>We have been working with a trusted partner who have written a specification of how exercising our backups could be delivered. We have submitted a PAG business case of which we awaiting the outcome to see if funding has been successful.</p> <p>To allow procurement of physical equipment (which is time dependent on suppliers), implementation and testing, request revised due date 31st December 2023</p>	31-Mar-2023
22 CS 06 Firewall event alerts	<p>Recommendation: Send firewall alerts to a shared mailbox to reduce dependency on a single individual. Retain the email as evidence that alerts were raised and record the action taken. For</p>	 60% MEDIUM RISK	Partially complete. Firewall alerts sent to shared mailbox. Work ongoing to integrate into new SIEM, Logging made easy dropped by the National Cyber Security Centre, Sophos integrations purchased and in the process of being implemented.	30-Apr-2022

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
	<p>example, use the alert email to automatically raise an event/incident in the service desk management system. The service desk system can record the alert life cycle and enable other operators to resolve the incident.</p> <p>Observation and implications: The firewall emails alerts to the Senior Technical Analyst's mailbox. A shared mailbox is not used. Alert emails are only retained for 7 days. Only the Senior Technical Analyst is informed of, and can act, on the firewall alerts. The short retention period makes it difficult to demonstrate that alerts were raised and acted upon.</p>		Request revised due date: 31st July 2023	
22 CS 10 Backup the firewall configuration	<p>Recommendation: Include backup of the firewall local certificates and the firewall configuration in the firewall operating procedures. Backup: - after any changes to the configuration - before any firmware upgrade Store copies of the firewall backups offline and physically remote from the firewall.</p> <p>Observation and implications: Manual backups are made using</p>	 <p>MEDIUM RISK</p>	<p>The firewalls are backed up. We are checking the certificate to see if it's possible to backup the configuration. We don't believe it is. The recommendation will be updated accordingly.</p> <p>To allow LAN2LAN to come to us to give a definitive answer, request revised due date: 31st July 2023</p>	30-Jun-2022

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
	<p>the firewall console backup utility. It is not clear if backup of the firewall local certificates is also performed or if the backups are secured off site. Reconfiguring the firewalls takes longer than recovering from backup. Recovery is needed if the firewall is reset to factory defaults or a TFTP firmware upload is performed. The firewall will not be able to inspect SSL/TLS traffic without the local certificates.</p>			
<p>22 CS 11 Restore from backup</p>	<p>Recommendation: Document restoring from backup in the firewall operating procedures. Schedule an exercise at the next planned firewall downtime, such as to upgrade the firmware. Use the lessons learned to improve the firewall operating procedures. Observation and implications: Restoring the firewall configuration from backup has not been exercised. Longer interruption of service and downtime whilst the firewall is restored or reconfigured.</p>	<p>0% MEDIUM</p>	<p>We have been working with a trusted partner who have written a specification of how exercising our backups could be delivered. We have submitted a PAG business case of which we are awaiting the outcome to see if funding has been successful.</p> <p>To allow procurement of physical equipment (which is time dependent on suppliers), implementation and testing, request revised due date 31st December 2023</p>	<p>04-Apr-2023</p>
<p>22 EM 01 A new Asset Management</p>	<p>Recommendation: A new Asset Management Plan should be drawn up, approved, and published. The</p>	<p>10%</p>	<p>Training Received on how to write a Management Plan, framework plan in progress & project team in place.</p>	<p>30-Apr-2023</p>



Code	Description	Progress Bar and Risk level	Latest Note	Due Date
Plan should be drawn up, approved, and published	<p>new Plan should be aligned closely with the Authority's Strategic Plan to ensure it will support and help deliver strategic priorities over the short to medium term.</p> <p>Observations: The Council does not have a current Asset Management Plan (AMP) and is therefore unable to take a proactive approach to managing its assets. The existing AMP is dated 2012-2016. Work is underway to create an updated plan to detail out the work required to maintain its assets, with the plan due to be completed by Summer 2023. This should support a more strategic and proactive approach to managing its assets along with the supporting Asset Management Strategy.</p>	HIGH RISK	Request extension of time: 30th September 2023	
22 EM 02 When new Asset Management system is in place implement a	<p>Recommendations: When the new system is in place implementing a fully interfaced database could avoid duplication of work.</p> <p>Observations: Limited administration support to maintain current systems in place, which is</p>	 <p>MEDIUM RISK</p>	<p>Revised Quote for TF upgrade and with Accountancy with approval and verification, confirming budgets in place.</p> <p>Request revised due date: 30th September 2023</p>	31-Mar-2023


Code	Description	Progress Bar and Risk level	Latest Note	Due Date
fully interfaced database	<p>exacerbated by the current database not fully interfacing with the Council's present finance system (Civica). This has been recognised by Management and the Terrier system is due for an upgrade.</p> <p>Harmonisation of software and hardware with a central database will improve officer efficiency and a fully interfaced database will give the Council an opportunity to consolidate data storage and report generation avoiding duplication.</p>			
22 EM 10 Condition surveys should be completed on all assets	<p>Recommendation: Condition surveys should be completed on all assets to give visibility of future maintenance commitments that are likely.</p> <p>Observation and Implications: Condition surveys are not conducted on all assets. A survey not only provides information for maintenance work that is required immediately. This survey also gives an indication of when future repairs, maintenance, decoration and renewal of each part of the building should be anticipated. Without</p>	<div data-bbox="857 1038 1059 1078" style="border: 1px solid black; width: 80px; height: 25px; display: flex; align-items: center; justify-content: center;">0%</div> <p>HIGH RISK</p>	<p>Our senior surveyor left NDC and we recruited internally but to date we have been unable to back-fill this position. We are currently advertising this role for a 2nd time. Once fully staffed we are committed to undertaking this new piece of work. Due to the number of assets we are requesting a year extension on the understanding that we will prioritise our largest assets.</p> <p>Request revised due date: 30th April 2024</p>	30-Apr-2023

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
	performing condition surveys on all assets, the Council is potential open to more major reactive work being needed in the future which could be prevented.			
22 EPCC 01 Develop an overarching response & Recovery plan to support the DEPP Plans.	<p>Observations & Implications: The Council relies on the generic plans produced by DEPP and does not have its own Emergency Plan. DEPP has told us that this is acceptable if officers are clear on their responsibilities and local circumstances. However, we consider that it would be better if the Council tailored this Emergency Plan to help direct officers in the event of an emergency.</p>	 <p>MEDIUM RISK</p>	<p>The revised National Planning Outage (NPO) project plan agreed at LRF Programme Board will require further work beyond the initial deadline of the end of August in order to complete the planning cycle and deliver an exercise to test the plan. The exercise is now expected to occur in September. However, the current LRF NPO leads secondment has finished and recruitment for a new lead is in progress, this may result in some delays in implementing the changes in government guidance and results of the debrief findings from exercise Mighty Oak. In addition the LRF manager has been seconded to a new post, so there are likely delays to programme of work.</p> <p>We continue to have DEPP response and recovery plans as well as an updated standby manual and specific risk plans to support any response in the meantime.</p> <p>Request revised due date: 22nd December 2023</p>	31-Dec-2022
22 EPCC 02 Once relevant	<p>Observations & Implications: The LRF provides an overall County</p>		An Emergency Planning and Business Continuity risk register is currently being drafted to analyse the risks	28-Feb-2023

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
risks from all sources have been collated, analysis of current plans & identification of any gaps in the planning process where further plans or mitigations would be beneficial	Risk Register listing the many county risks that may arise. As well as the generic DEPP central plan, the Council holds a variety of other plans such as the Rest Centre Plan, Operation London Bridge, and Ilfracombe Harbour Oil Spill Contingency Plan to help manage these risks. We consider there would be benefit in the Council considering whether the range of plans are sufficient and cover the significant risks considered most relevant to North Devon.	MEDIUM RISK	<p>from the community risk register, national security risk assessment and horizon scanning documents with the aim of identifying what plans (National, LRF, DEPP, NDC) are currently in place and what additional mitigation measures may be required.</p> <p>The delay in completing this work is due to awaiting updated risk assessments, the LRF has now received the revised NSRA and National Planning assumption and these were issued at the end of May. The LRF risk working group will now need to consider these risks for the locality and this will inform local risk assessments and community risk register. It is not clear what the timeline for this work will be.</p> <p>The progress of the risk register can be viewed on corporate drive > Silver and can be viewed by senior management who require it for planning purposes, this is due to the sensitivity level of the NSRA.</p> <p>Request revised due date: 31st October 2023 to allow time for the LRF RAWG to review the changes and pass this information along to partners. this document will remain live and will be updated as necessary but this action can be closed as a process will be in place to review risks in the area and consider where mitigations would be beneficial.</p>	

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
22 PO 06 Risks relating to the Car Parking service should be reviewed	<p>Recommendations: Risks relating to the Car Parking service should be reviewed as the date recorded as last assessed upon Pentana Risk was two years nine months previously.</p> <p>Observations: Risks are recorded upon 'Pentana Risk' held upon the North Devon Council system. Three risks are shown against Car Parks upon the Service Risk Register: -</p> <ul style="list-style-type: none"> • Loss of Local Decision Making on Parking; • Revenue Budgets; • Loss of Income The date they were last assessed is detailed as 28 February 2020. 	<div style="border: 1px solid black; width: 100px; height: 20px; margin-bottom: 5px;"></div> <p>0%</p> <p>MEDIUM RISK</p>	<p>Due to staff absence a further update is currently unavailable, request a short extension to ensure review has been completed.</p> <p>Request revised due date: 30th June 2023</p>	31-Mar-2023
22 RRS 01 Review Recruitment Policy	<p><u>Recommendation:</u> The Policy should be reviewed and brought up to date with a current version number and reviewable on date.</p> <p><u>Observation and Implications:</u> Recruitment Policy is out of date(effective June 2016)with the risk that is no longer up to date with current legislation and best practice.</p>	<div style="border: 1px solid black; width: 100px; height: 20px; background-color: #ccccff; margin-bottom: 5px;"></div> <p>80%</p> <p>MEDIUM RISK</p>	<p>This policy has been drafted and circulated to Unison for comment.</p> <p>Short Extension of Time Request: 30 July 2023</p>	31-Mar-2023

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
22 S 02 Consider member involvement in the review of the arrangements for Safeguarding Policy	<p>Recommendation: The extent of member involvement and visibility of the effectiveness of Safeguarding arrangements in the council should be considered during review of the Policy.</p> <p>Observations and Implications: Safeguarding arrangements, and specific performance is not communicated to Members as described in the Policy. There is a risk that Safeguarding developments at NDC are not known at Member level for which they are accountable.</p>	 0% MEDIUM RISK	<p>It is proposed safeguarding could be incorporated into the Community Safety lead role.</p> <p>Request extension of time until the 30th June 2023.</p>	31-Dec-2022
22 S 03 Refresher training for members, SMT and lead officers	<p>Recommendation: Undertake refresher training for members, senior management and lead officers.</p> <p>Observation and Implications: Plans in place to deliver PREVENT training and links provided show action being taken. However, it is now three years since policy and training delivered on remainder (besides County Lines delivery in July) so refreshers would be advisable for Members, Senior Management and Lead Officers.</p>	 90% MEDIUM RISK	<p>Member training for safeguarding scheduled for July (this will also incorporate community safety).</p> <p>Safeguarding refreshers for all staff, including SMT & Lead Officers are being organised in June with the training taking place shortly afterwards.</p> <p>Request short extension of time: 31st July 2023</p>	28-Mar-2023

Code	Description	Progress Bar and Risk level	Latest Note	Due Date
<p>22 TLSC 01 The screed depth around the pool is thinner than agreed as part of the contract specification</p>	<p>Recommendation: A suitable resolution to the issue should be obtained. Observation and Implications: One of the potentially more significant defects yet to be resolved relates to the screed depth around the pool which is thinner than agreed as part of the contract specification. There is understood to be no direct financial risk to the Council associated with this issue, as responsibility for this lies with Parkwood and their subcontractor Speller Metcalfe, at least for the initial 20-year contract period. Any future closure of the facilities however, to rectify issues arising from this issue, may carry reputational risk and lead to lost income.</p>	 <p>MEDIUM RISK</p>	<p>This issue is on the snagging list for the project. The screed depth varies from that specified, is thought to be fine, but should have gone through a derogation process before being agreed. For that reason, there is a project requirement for the contractors to produce a warranty for the works. This should be resolved by the end of the snagging period which is end June 2023.</p> <p>Request for a short extension of time: 30th June 2023</p>	<p>31-May-2023</p>