ADUR & WORTHING
COUNCILS

Joint Audit and Governance Committee
Date: 18/01/2024

Key Decision [No]

Ward(s) Affected: All

Disaster Recovery Plan

Report by the Director for Sustainability & Resources

Officer Contact Details
Name: Adam Saunders
Role: Head of Technology & Design
Email: adam.saunders@adur-worthing.gov.uk

Executive Summary

1. Purpose

This report outlines the comprehensive journey undertaken to develop and implement the Disaster Recovery Plan (DRP) for the council's systems. The process involved assessing the existing systems, their contracts and collaborating with system owners to establish robust recovery procedures.

2. Recommendations

To review and acknowledge the completion and launch of the new IT Disaster Recovery Plan

3. Context

3.1. What is a DR plan?

3.1.1. A Disaster Recovery Plan (DRP) is an integral component of an organisation's broader business continuity strategy. It's designed to enable quick and efficient recovery from various types of disasters that can impact IT infrastructure and data, such as natural disasters, cyberattacks, hardware failures, or human error. The plan encompasses more than just data backup and recovery; it includes a range of strategies and procedures to maintain or quickly resume critical business functions.

3.1.2. Key aspects of a comprehensive DRP include:

- Risk Assessment and Management
- Identification of Critical Systems and Processes
- Data Backup and Recovery Solutions
- Communication Plan
- Regular Testing and Updates
- Employee Training and Awareness
- Business Impact Analysis (BIA)

3.2. Audit Background

3.2.1. During the fourth quarter of 2021, Mazars conducted an audit focused on the IT Disaster Recovery Plan.

3.2.2. The final report, dated July 2022, contained priority one recommendations and management responses.

3.2.3. It was broadly recognised that the audit findings necessitated a complete overhaul of the existing DR Plan. This redesign was to be a collaborative effort between the Digital team and the Safety and Resilience Manager.

3.3. Digital Team & Policies Background

3.3.1. Adur and Worthing Councils' Digital team was initially part of a shared IT service called "CenSus."

3.3.2. CenSus provided IT support to several local authorities, including Horsham, Mid-Sussex and Adur & Worthing. The transition from this shared support to internal teams began in 2017, leading to the establishing of a new in-house Digital team as part of a larger

reorganisation.

3.3.3. With the formation of the new internal Digital team, all existing Digital policies and DR Plans, previously managed by CenSus, needed to be updated and republished under the ownership of Adur & Worthing Councils. The transition and updating of these Digital policies commenced in 2021/2022.

3.4. Key issues

3.4.1. A significant challenge in reviewing, updating, and republishing all 21 new Digital Policies, along with the Disaster Recovery (DR) Plan, was the strain on resources. This task required the same team members already engaged in providing essential break-fix services to staff, creating a substantial workload.

3.4.2. To alleviate the resource burden and accelerate the progress, we successfully applied for the Local Digital Cyber Fund through the Department for Levelling Up, Housing and Communities (DLUHC). This application secured £100,000 in external funding and was allocated during the 2022/2023 Financial year.

3.4.3. The Cyber grant funds have been allocated for the hiring of an Information Security Officer on a Fixed Term Contract for one year. This appointment has been recorded in the Digital Risk Register, highlighting the need for additional funding approval to continue this crucial position. The long term goal is to make this role permanent through a growth bid.

3.4.4. Additionally, the funds facilitated the procurement of a new Information Security Management System (ISMS) for a two-year period. These steps were pivotal in enhancing our capabilities to update and manage our digital policies and DR Plan effectively.

3.4.4.1. *ISMS.online is a digital tool streamlining policy creation and management, offering ISO27001-aligned guidelines and ready-made templates. It supports team collaboration and tracks policy changes, ensuring compliance with legal and industry standards. The platform facilitates identifying and managing security risks and keeping policies updated and accurate. Additionally, it provides auditors with the necessary access for reviewing information for compliance purposes and aids in staff training for effective policy implementation and adherence.*

4. Issues for consideration

4.1. DR Plan Creation Process

4.1.1. In Q3 2022, initial scoping for a new Disaster Recovery (DR) Plan, as recommended by the audit, revealed its complexity and significant resource demands.

Limited Internal Knowledge:

4.1.2. The limited comprehensive centralised knowledge about documented systems, hosting details, contract owners, existing DR plans, and backup and restore procedures was a significant hurdle. Understanding these elements was crucial in drafting an accurate and implementable DR Plan.

System Assessment:

4.1.3. The initial step required a detailed analysis of all systems within the councils. This involved collaboration across multiple departments – Digital, Services, Legal, Procurement, and Safety and Resilience.

4.1.4. A detailed inventory was then created including the criticality of recovery in a DR situation. The systems were broken down into 18 critical, 8 medium, and 12 low priority, determining their recovery criticality in a DR scenario.

Contractual Review:

4.1.5. A thorough review of contracts with third-party suppliers was conducted to assess DR provisions. This revealed gaps in many agreements, necessitating existing and new contract amendments to ensure inclusion and awareness of DR requirements. This is an ongoing process.

4.1.6. A new cyber security checklist questionnaire has been agreed upon and launched, being sent to all existing suppliers, and is part of all new Digital procurements in the future.

Identifying System Owners:

4.1.7. Identifying and collaborating with system owners was pivotal. This facilitated gathering essential information and assigning accountability for each system's recovery process.

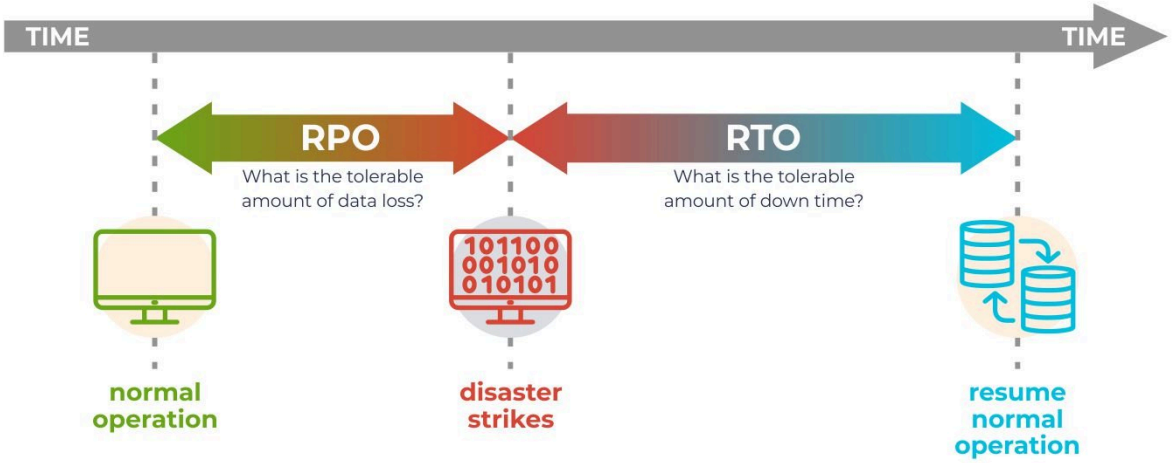
Documenting Recovery Procedures

4.1.8. Recovery procedures for each system/server were documented in collaboration with system owners and third-party suppliers. This included defining the Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for each system, which is essential

for establishing effective recovery strategies.

4.1.8.1. **RPO (Recovery Point Objective):** Measures the maximum tolerable period of potential data loss.

4.1.8.2. **RTO (Recovery Time Objective):** Indicates the maximum allowable time for restoring a system or service after an incident.



4.2. Ongoing Maintenance of the *IT Systems - Disaster Recovery Plan*

4.2.1. The IT Systems - Disaster Recovery Plan is a dynamic document, necessitating continuous review and updates by the Digital team and the Safety and Resilience manager. This ongoing maintenance is critical for several reasons:

4.2.2. **Adapting to Technological Evolution:** As new systems are implemented, they bring new recovery challenges and requirements. The DR Plan must incorporate these to ensure comprehensive disaster preparedness.

4.2.3. **Decommissioning of Outdated Systems:** When old systems are phased out, the DR Plan must be revised to remove redundant recovery procedures, ensuring focus on current infrastructure.

4.2.4. **Changes in System Hosting and Recovery**: Modifications in how existing systems are hosted or recovered can significantly impact disaster recovery strategies. The DR Plan must reflect these changes to ensure effective recovery.

4.2.5. **Updating RTO/RPO Metrics:** Regularly revising Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) ensures they align with the current operational capabilities and business continuity requirements.

4.2.6. **Ensuring Compliance and Risk Management:** Continuously updated DR Plans help adhere to industry standards and regulations. It also plays a crucial role in risk management by preparing for potential disruptions.

4.3. IT Disaster Recovery Plan Implementation

4.3.1. Following the completion of the preliminary stages outlined in sections 4.1 and 4.2, we successfully developed and put into action a detailed IT Disaster Recovery Plan.

4.3.2. This plan was fully operational as of September 2023.

4.3.3. In the fourth quarter of 2023, we presented the finalised DR plan to Mazars for a thorough evaluation as a component of a broader assessment of our Digital Policies. Mazars, in collaboration with our Digital team, conducted a preliminary wrap-up meeting on 20th December 2023 to discuss the audit findings.

4.3.4. We anticipate receiving a preliminary draft of the audit report from Mazars in the first week of January 2024. As of this report's composition, the initial feedback from Mazars has been encouraging, indicating that our new DR Plan meets all the essential criteria. However, some minor amendments will need to be considered.

5. Engagement and Communication

5.1. An integral component of developing the Disaster Recovery (DR) Plan for Adur & Worthing Councils has been robust engagement and communication across various departments and stakeholders. This collaboration was essential not only in pooling knowledge and resources but also in ensuring a comprehensive understanding and alignment with the councils' operational needs, risks and potential business impact should a Disaster occur.

Stakeholder Engagement:

5.2. Key stakeholders were actively involved, including system owners, legal, procurement teams, and third-party suppliers. This engagement was crucial in identifying and documenting system-specific requirements, understanding contractual obligations, and ensuring adherence to disaster recovery protocols.

Communication Strategy:

5.3. A clear and consistent communication strategy was adopted to keep all parties informed and involved. Regular updates, meetings, and collaborative workshops ensured transparency and fostered a sense of shared

responsibility towards the DR Plan's success. The safety and resilience manager worked collaboratively to ensure that the DR plan enhanced the Business Continuity Plan rather than conflict with it.

Feedback and Input:

5.4. Feedback from various departments was actively sought and incorporated. This participatory approach ensured that the DR Plan reflected different council functions' diverse perspectives and operational risks.

Training and Awareness:

5.5. Comprehensive training sessions were conducted. These sessions aimed to educate Digital staff about the importance of disaster recovery, familiarise them with the DR Plan, and clarify their roles in its implementation. Further work is required to ensure the success of the implementation.

6. Financial Implications

There are no financial implications from this report. The additional costs incurred to progress the Disaster Recovery Plan have been funded through the Local Digital Cyber Fund following a successful bid to the Department for Levelling Up, Housing and Communities (DLUHC).

7. Legal Implications

This report is for noting. Therefore, no specific legal implications arise from the report at this stage.

Background Papers

None

Sustainability & Risk Assessment

1. Economic

1.1. An effective IT Disaster Recovery (DR) Plan is crucial for maintaining economic stability and growth. In a system failure or cyberattack, a well-prepared DR Plan minimises downtime, safeguarding public and private sector operations. This ensures continued economic participation and prevents significant financial losses. Conversely, the absence of a robust DR Plan could lead to extended service disruptions, eroding trust in local businesses and government, potentially deterring investment and economic development.

2. Social

2.1. Social Value

A comprehensive DR Plan contributes to community confidence in public services, reinforcing the perception of a responsible and proactive council. It ensures the continuity of essential services, which is particularly crucial for vulnerable groups who rely heavily on these services.

2.2. Equality Issues

An effective DR Plan ensures equitable access to council services, especially during crises. It guarantees that all community members, regardless of their background or abilities, have uninterrupted access to critical services.

2.3. Community Safety Issues (Section 17)

A robust DR Plan is integral to maintaining public order and safety. It ensures that critical data and services related to crime and disorder reduction are always available, thus supporting the Council's duties in these areas.

2.4. Human Rights Issues

A well-implemented DR Plan respects individuals' rights by protecting personal data and ensuring the continuity of services that support their daily lives. The plan's proportionality and necessity are justified under the Human Rights Act, especially considering the right to privacy and protection of personal information.

3. Environmental Impact

An effective DR Plan can include environmentally sustainable practices, such as prioritising cloud-based solutions to reduce the physical footprint of IT infrastructure.

4. Governance

4.1. Alignment with Council Priorities: A DR Plan aligns with the Council’s transparency, accountability, and service reliability priorities. It's a fundamental part of risk management and operational continuity strategies.

4.2. Reputation and Partnerships: The presence of a reliable DR Plan enhances the Council's reputation as a dependable and responsible entity, fostering trust among partners and communities.

4.3. Resourcing and Risk Management: Implementing a DR Plan involves assessing resource allocation to ensure operational readiness. It addresses health and safety risks by safeguarding critical data and systems, which are essential for emergency response and public safety.

4.4. All operational Digital technology, Cyber, Digital Policies and Digital Plans are reported to the Technology and Information Board