http://doi.org/10.7207/twgn26-02

Cyber Security and Resilience for Digital Preservation

Part 2: Engage Stakeholders

Heather Lowrie and Garth Stewart

DPC Technology Watch Guidance Note

July 2026

DigitalPreservationCoalition

ISSN: 2048-7916

This report is published by the Digital Preservation Coalition (DPC). The DPC is an international charitable foundation which supports digital preservation and helps its members around the world to deliver resilient long-term access to digital content and services. In addition to the publication of reports on a range of themes which cover the state of the art in digital preservation, the DPC also supports its members through community engagement, targeted advocacy work, training and workforce development, identification of good practice and standards, and through good management and governance. Its vision is a secure digital legacy.

Discover the DPC's publications, including the latest updates and revisions, at:
https://www.dpconline.org/digipres/discover-good-practice/tech-watch-reports

Find out more about the DPC, the support it offers and how to become a member at:
https://www.dpconline.org/about/join-us

DPC Cyber Security and Resilience Guidance Note Series

Organizations that carry out digital preservation activities operate in an increasingly hostile cyber environment. Threats have grown in frequency, scale, and sophistication, placing unique and irreplaceable collections at risk. Sadly, it is now a case of - *not if, but when* - any organisation holding digital collections of long-term value is subject to cybercrime.

This creates pressure on digital preservation practitioners to understand this issue to a reasonable level of detail and identify key cyber threats to their collections. It is rare that practitioners will be able to confront these threats alone: collaboration and engagement with other teams such as IT will be a likely key next step. This collaboration should lead to the application of appropriate cyber security measures that protect digital collections as far as possible and enable response to a cyber-attack.

However, cyber security is a challenging, often overwhelming subject, especially for practitioners who may have limited time and resources yet need to understand the following areas:

1. Where to begin with a subject like this: what are the risks?
2. What successful pathways towards engagement look like.
3. How to put plans into action so that attacks can be neutralised, impacts can be mitigated, and recovery is possible.

The DPC has published a set of three Guidance Notes to support practitioners in this effort. They will support practitioners and organizational leaders in developing effective responses while maintaining business continuity and safeguarding staff wellbeing. They also encourage organizations to embed cyber security within digital preservation governance and operational practice in ways that protect collections while enabling usability, access, and long-term resilience.

This Guidance Note is the second in the series and focuses on engaging stakeholders. Note that technical terminology is defined within the Glossary.

1 Introduction

Digital preservation is most effective when all stakeholders are actively engaged, informed, and supportive. The same principle applies to cyber security for digital preservation. Security within digital preservation requires strong stakeholder engagement. However, before considering these stakeholders, it is important to first focus on the role of digital preservation practitioners themselves.

2 Role of digital preservation practitioners

Digital preservation practitioners play a key role in implementing cyber security within digital preservation environments. This can involve translating domain-specific concepts and requirements for wider stakeholder groups, while also interpreting cyber security principles back into preservation practice. In this sense, the role can extend to that of a 'change agent', bridging the gap between digital preservation needs, strategic oversight, and operational implementation. Key responsibilities may include:

- **Communicating risks and mitigations** to teams in understandable, actionable terms.
- **Supporting professional judgement** while ensuring accountability and adherence to governance frameworks.
- **Facilitating collaboration** between preservation staff, IT, and security teams to ensure alignment on priorities and organizational risk appetite.
- Working across all of these groups to **embed security policies** into day-to-day preservation workflows without compromising usability or innovation.
- **Monitoring emerging threats** and guiding teams in adopting new tools, technologies, or practices safely.

2.1 Digital Leadership

The responsibilities listed above are significant and may well require time to understand and apply. One emerging professional development concept that practitioners may find helpful are digital leadership capabilities. These include:

- Being clear about purpose and organizational objectives.
- Fostering innovation and experimentation within safe boundaries.
- Championing and managing change effectively.
- Using data and risk management approaches to inform decision-making.
- Maintaining an appropriate level of technical fluency to engage meaningfully with technical stakeholders.

These capabilities may take time to develop and may not all be necessary. However, practitioners working on the interface between digital preservation and cyber security, may wish to look out for appropriate training and development opportunities covering these areas (OECD, 2021, Lopez-Figueroa, 2025, Collins & Evans, 2007).

By combining professional expertise with proactive collaboration, digital preservation practitioners may find they are able to quickly foster trust with IT and information security teams. This can create many benefits: providing a suitable environment for collaborating, designing and embedding cyber security measures into day-to-day preservation operations while maintaining scope for future innovation, as well as generating trust and support structures for practitioners across their

organization. These connections can be a source of cohesion, understanding, and resilience when navigating further change and security incidents as required.

2.2 Mental health and wellbeing

The DPC's *Mental Health and Wellbeing Report*, published in 2025 highlighted the significant impact of the digital preservation advocacy burden on the mental health and wellbeing of practitioners as well as unclear roles and responsibilities and unrealistic workloads (Digital Preservation Coalition, 2025).

Practitioners should ensure that they know how far their own responsibilities and/or level of expertise in this area extends and when they require the support of others. It can be helpful to use tools such as corporate risk registers to ensure resources, capacity and staff wellbeing is kept in clear focus with appropriate leadership accountability, and that these factors remain explicitly considered in planning and decision-making.

Critically, practitioners must not try to tackle this subject alone. They should request regular training in cyber security if this is not already provided and advanced training if required. If any concerns arise, these should be reported or escalated promptly through appropriate channels. Practitioners have the right to a safe and healthy working environment, where both physical and mental health is protected and promoted. This is very much a health and safety matter: where leadership plays a critical role. (ILO, 2022)

3 Engaging Leadership and Governance

Acquiring and sustaining leadership support for cyber security and resilience for digital preservation is important but may be challenging. Leadership will likely have many risks and responsibilities to oversee: crafting an effective advocacy approach to this is hugely important. The following may help.

3.1 Remind leadership this is their responsibility

Cyber security for digital preservation is fundamentally a leadership responsibility. It cannot and must not be delegated solely to preservation staff, technical teams, or treated as a purely operational concern. Effective leadership ensures that preservation systems, which safeguard unique, irreplaceable digital collections, are recognised as critical organizational infrastructure, and supported accordingly through investment and resourcing.

Leaders must provide clear authority, dedicated resources, and strategic oversight, integrating cyber risk management into digital preservation governance, policy, and decision-making processes as appropriate. By doing so, they can create the conditions for staff to work safely, responsibly, and creatively. If leadership themselves require more guidance in cyber risk, resources are readily available for non-specialist audiences (NCSC, 2025).

3.2 Measuring progress: what to aim for

Advocating for leadership to own this responsibility can be challenging and senior support is not always guaranteed.

The intangibility and complexity of digital preservation are common obstacles to understanding and partnership, though strong public resources to support advocacy are available (Digital Preservation Coalition, 2026, Digital Preservation Coalition, 2026). Agreeing on adequate security controls and success criteria on top of that can be a challenge. At the same time, the growing and demonstrable threat posed by cybercrime provides a strong basis for advocacy, urgency, and organizational alignment: the time to act is now.

The following list outlines practical approaches and key arguments that may support this. Applying these to organizational contexts may help define and measure progress in cyber security and resilience for digital preservation, whether these be documented in a digital preservation policy; risk register, or mission statement:

- **Recognise the strategic importance of digital preservation systems**: Digital repositories and associated tools are essential infrastructure. Without these the digital record of current times will be lost. Their compromise to cybercrime could have lasting cultural, legal, and reputational consequences. Ensure that these messages are shared with leadership.
- **Assign senior ownership**: Designate a responsible executive with clear authority and accountability for digital preservation cyber security, supported by sufficient staff, funding, and technical expertise.
- **Integrate cyber risk into governance structures**: Include digital preservation security in organizational risk registers, reporting cycles, and audit frameworks to ensure oversight at the highest level.
- **Foster a security-conscious, high-trust culture**: Encourage transparency, professional judgement, and responsible risk-taking, so that staff feel empowered to act safely without fear of blame. One method to develop this is the use of a Zero Trust framework (see section 3.3).
- **Understand the severity of threats which cybercrime imposes on digital preservation and make duty of care to staff a priority:** managing digital preservation and cyber security is complex, often pressurised work. Leadership must fully understand this, and invest in a suitable resourcing model, with clear, agreed roles and responsibilities.

3.3 Zero Trust Thinking: cementing a high-trust culture for digital preservation

Digital preservation can introduce new cybersecurity risks that may create understandable concern for leadership and governance structures. Conversely, if implemented in line with good practice and with adequate, sustained resource, digital preservation can be a help not a hinderance, to cyber security and resilience.

One approach that could address this hesitation and strengthen cross-organizational partnership is the adoption of Zero Trust architecture principles as a guiding framework for stakeholder engagement.

Originating within the cyber security community, Zero Trust principles, summarised as ‘never trust, always verify’, are well suited to designing and managing digital preservation environments and workflows. Rather than assuming that systems, users, or network components are inherently trustworthy, Zero Trust treats all access requests and operations as potentially risky and therefore requires continuous verification at every stage of interaction (NIST, 2020). Further information is available from the UK’s National Cyber Security Centre on their website (NCSC, 2026).

A critical aspect of Zero Trust architecture is that it applies to systems and access pathways, not people. This distinction is crucial in digital preservation contexts, where success so often relies on a strong culture of professional judgement, collaboration, and mutual trust. It is a culture in which practitioners should feel empowered to make informed decisions, report concerns, and innovate safely without fear of blame by leadership.

When used as a guiding framework for digital preservation and cybersecurity alignment, Zero Trust can help reinforce this culture in several practical ways:

- **Encourage open reporting**: Create channels for staff to flag risks, anomalies, or near misses without fear of punitive consequences.
- **Respect expertise**: Recognise the specialised knowledge of all professionals to the cause and involve them in risk assessment and security planning.
- **Provide training, time, and resources**: Equip staff with the knowledge, tools, and capacity to work securely while maintaining operational efficiency.
- **Allow for learning from incidents**: Use security events as opportunities to improve systems, processes, and workflows rather than assign fault.

In practice, security controls should function as safety guardrails, guiding and protecting staff, rather than as mechanisms of surveillance or control. A takeaway message for leadership: when Zero Trust principles are combined with a high-trust professional culture, organizations can achieve both strong security *and* operational resilience: enabling the safe and sustainable preservation of irreplaceable digital collections. In this model, cybersecurity becomes a **shared responsibility:** embedded within digital preservation culture and workflows, rather than imposed as an external constraint.

4 Working with IT

The essential requirements of digital preservation can create a complex 'attack surface' for cybercrime. When designing preservation workflows and systems, the first steps are to clearly communicate requirements across the organization and build a strong working relationship with IT and information security colleagues. Ideally, this will enable **co-design** of digital preservation infrastructure: workflows and processes that contain security controls that appropriately mitigate risks, yet proportionally enable innovation and the secure processing of potentially hazardous material.

4.1 Approaching conversations with IT

Working with IT on cyber security is a critical factor for success. Here are some key points to bear in mind:

- **Approved exceptions, constraints and mitigations to standard IT policies** should be documented, justified, and formally governed to maintain accountability.
- Building on Zero Trust, **professional judgement should be respected** within clear accountability frameworks, recognising the expertise of preservation and IT staff.
- If **test environments** are required as part of a workflow, containment, network segmentation, and monitoring are typically more effective than outright bans in managing operational risk. Blanket prohibitions, for example for the development of authorised 'sandbox' test environments, can drive user activity into unmanaged or undocumented spaces, increasing overall risk rather than reducing it.
- Be clear on **who requires access** to restricted networks, tools and applications, what their skills are in working with these, and whether any additional training and/or certification is required.

- Aim to **frame preservation needs** in terms of organizational risk, value, and mission impact, rather than purely technical requirements.
- Involve IT and security teams **early** in system design, procurement, and workflow planning.
- Establish **regular communication** channels, rather than relying on one-off consultations, to ensure ongoing alignment and mutual understanding.

4.2 NIST: Using standards to reach common language and understanding

It is critical to define agreed terms and shared semantics when communicating with IT and cybersecurity colleagues during co-design discussions (Prater, 2018). Language is key. The use of recognised professional models such as the DPC's Rapid Assessment Model (RAM) (Digital Preservation Coalition, 2024) and the NDSA Levels of Preservation (NDSA, 2026) can be extremely useful in establishing mutual understanding. A similar approach can be applied to cybersecurity. The US National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2024) provides a widely adopted structure for managing and improving organizational security. It aligns well with digital preservation practice and is familiar to cybersecurity professionals, making it a valuable tool for facilitating productive communication between preservation teams, IT departments, and security colleagues.

By framing cyber security in terms of the framework's six core functions, preservation practitioners may be able to better articulate risks, requirements, and mitigation strategies in ways that resonate with IT and cyber security professionals. The key pointers for digital preservation practitioners are indicated below.

4.2.1 Govern

Definition: Governance ensures that cyber risk in digital preservation is treated as a strategic priority. This topic has been covered (see section 3).

4.2.2 Identify

Definition: Identifying assets, dependencies, and risks is essential for informed decision-making and structured risk management. For digital preservation, collaboration may focus on:

- Maintain up-to-date **inventories** of digital assets, repositories, and preservation tools and applications.
- Map internal and external **dependencies**, including cloud services, vendor platforms, and open-source tools. When necessary, apply further security measures such as IP-locking to ensure preservation systems can only be accessed from trusted machines, or use of a Single Sign On to systems in place of the more vulnerable username/password mechanism. Collaborate to ensure implementation of dependencies follows good practice (NCSC, 2023).
- **Classify data** according to sensitivity, legal obligations, and preservation requirements. This assessment will inform decision-making on other infrastructure considerations (for example, type of storage user, whether it is safe to use Web-facing applications for preservation tasks such as data analysis, access interface functions).
- Conduct preservation-specific **risk assessments** to understand threats associated with content, workflows, and technology. Articulate these risks and review frequently – at least every 3 months. Community frameworks for calculating digital preservation risk such as CHARM and DiAGRAM may be useful to this exercise (Pennock, 2024, The National Archives (UK), 2021).

4.2.3 Protect

Definition: Protection measures are designed to prevent or reduce the impact of security incidents.

- Work with IT to implement **strong authentication and access controls**, including role-based permissions. Keep all parts of the digital preservation environment in mind here – including any associated APIs, application integrations, and communication/support portals. It may be helpful to adopt the principle of least principle when deciding on role-based permissions to systems and applications (NIST, 2026).
- Apply **encryption** for data in transit and at rest, balancing security with long-term accessibility. Options could include HTTPS and SFTP.

4.2.4 Detect

Definition: Early detection of anomalies and threats is essential to maintaining integrity and trust.

- Practitioners should ensure they receive adequate **reporting** from IT on access logging, user activity and potential security events as appropriate. **Fixity checking** to monitor for unintended changes or corruption is standard practice for digital preservation: but will also **directly enhance system monitoring efficacy.** This is a powerful advocacy message for digital preservation practitioners.
- Deployment of suitable **anti-virus protections** are key. Work with IT to use multiple anti-virus software engines where feasible, at all major stages of preservation (transfer, ingest, access, and on a standard semi-regular basis as appropriate to counter zero-day events). Update these tools as and when required – as the threat landscape changes, it is critical that tools correspond with the latest intelligence on threats. Note that **the depth of anti-virus-scanning** should be carefully considered. Digital preservation often involves the handling of large, compressed container file formats such as .zip, .tar, .warc, containing multiple associated files. It may be necessary to 'unpack' the full contents of these container files for comprehensive, individual file-level scanning.

4.2.5 Respond

Definition: response planning ensures that incidents are managed effectively and consistently to minimise impact. There is much to consider for digital preservation practitioners, dependent on organizational context. Reach out to IT colleagues for further advice, but key considerations may include:

- Develop **incident playbooks** tailored to preservation-specific scenarios, such as ransomware or supply chain compromise.
- Define **containment strategies** to isolate affected systems while maintaining overall repository integrity.
- Prepare internal and external **communication plans** for stakeholders, partners, and donors.
- Regularly **test response procedures**. Examples could include independent penetration tests of systems by a trusted third party, testing of disaster recovery procedures and interrogation of log files.

4.2.6 Recover

Definition: Recovery focuses on restoring services and strengthening resilience after incidents. Again, digital preservation good practice can support this phase:

- Maintaining **independently managed, geographically distributed copies** of digital content, ideally on varied storage technology is a building block of digital preservation (DPC, 2022). This configuration can be of direct benefit to recovering from a cyber-attack as having separate, isolated copies provides much greater redundancy. Copies of lost or corrupted content could be swapped in from isolated, unaffected collections, enabling 'healing' of content.
- Options for **offline, physical storage** technologies such as tape, DNA and silica storage offer further protections against cybercrime (Library of Congress, 2026, Daly, 2024, NDSA, 2026).
- Other considerations include **planning for resumption** of digital preservation workflows with predicted timescales for recovery, **post-incident review** to capture lessons learned and improve future safeguards, and **sharing of these insights** with the wider digital preservation community to **strengthen collective resilience**.

NIST provides a potential framework for combining cyber security and digital preservation requirements, procedures, and responses, for better coordination and resilience. Depending on jurisdiction and organizational context, additional standards and frameworks may also be relevant; including ISO/IEC 27001 (ISO, 2013), Cyber Essentials Plus (NCSC, 2026), Secure by Design principles (GSG, 2026), the Australian Information Security Manual (ASD, 2026), and CIS Benchmarks (CIS, 2024).

5 Conclusion

Engaging on cyber security and resilience for digital preservation will require careful consideration, delivery, and patience. It is hoped that the guidance above provides practitioners with ideas on how to get started, and suitable arguments and cases to craft. As can be seen from the NIST framework analysis, if carried out carefully and effectively, in line with good practice, digital preservation can not only complement any cybersecurity programme (via fixity monitoring, anti-virus controls, format analysis), but bolster it through additional redundancy (multiple, independently managed copies). This may be the fundamental point on which to base strong stakeholder engagement. In our final Guidance Note in this series, we take this concept further through practical examples.

6 Glossary

Attack surface: The sum of vulnerabilities, pathways, or methods—sometimes called attack vectors—that hackers can use to gain unauthorized access to an organization's network or sensitive data, or to carry out a cyber-attack.

Encryption: A security process that converts readable data (plaintext) into unreadable code (ciphertext) using algorithms and keys, so that only authorized parties can access the original information.

HTTPS: A method for encrypting the content of a webpage between servers and a user's browser; and protecting user input on a website or mobile applications, or both.

Incident Playbook: A documented, step-by-step guide that outlines procedures and responsibilities for responding to specific types of cybersecurity incidents (for example ransomware attack, data breach).

Integrity: That information contained within digital content remains accurate and complete.

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to systems. Examples include viruses, worms, ransomware, spyware, and trojans.

Ransomware: A type of malware which prevents access to devices and data stored on these, usually by encrypting files. A criminal group will then demand a ransom in exchange for decryption.

Sandbox: An isolated and controlled environment used to safely test software or analyze suspicious files without affecting the main system.

Single Sign On (SSO): An authentication scheme that lets users log in once using a single set of credentials and access multiple applications during the same session.

SFTP: Stands for secure file transfer protocol, used to transfer files securely over a network.

Zero-Day Events: Where an attacker takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware, in order to spread malware or access sensitive information. 'Zero day' refers to the fact that the software or device user has zero days to fix the flaw because attackers can already use it to access vulnerable systems.

7 References

Australian Signals Directorate (ASD), 2026. *Information security manual*. Canberra: Commonwealth of Australia. Available at: https://web.archive.org/web/20260618033453/https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism

Center for Internet Security (CIS), 2024. *Critical Security Controls*. East Greenbush: CIS. Available at: https://web.archive.org/web/20260705021427/https://www.cisecurity.org/controls/

Collins, H., & Evans, R., 2007. *Rethinking expertise*. Chicago: University of Chicago Press.

Daly, S., 2024. *A decoupled Custodial Copy for cloud-based Digital Preservation Systems.* London: UK Gov. Available at: https://web.archive.org/web/20260708102055/https://www.digipres.org/publications/ipres/ipres-2024/papers/a-decoupled-custodial-copy-for-cloud-based-digital-preservation/

Digital Preservation Coalition (DPC), 2026. *Digital Preservation Advocacy Toolkit.* London: DPC. Available at: https://web.archive.org/web/20260708102406/https://www.dpconline.org/digipres/champion-digital-preservation/digital-preservation-advocacy-toolkit

Digital Preservation Coalition (DPC), 2024. *Digital Preservation Coalition Rapid Assessment Model (DPC RAM)*. Version 3. London: DPC. Available at: https://web.archive.org/web/20260504122325/https://www.dpconline.org/docs/digital-preservation/ram/3123-digital-preservation-coalition-rapid-assessment-model-v3/file

Digital Preservation Coalition (DPC), 2022. *Digital Preservation Handbook*. 2nd Edition. London: DPC. Available at: https://web.archive.org/web/20260604135805/https://www.dpconline.org/handbook

Digital Preservation Coalition (DPC), 2025. *Mental Health and Wellbeing in the Digital Preservation Community: 2023 Survey Findings Report.* London: DPC. Available at: https://web.archive.org/web/20260708103814/https://www.dpconline.org/docman/digital-preservation/mhw/3431-mhw23-report/file

Digital Preservation Coalition (DPC), 2026. *Novice to Know-How: Advocacy.* London: DPC/The National Archives. Available at: https://dpc.getlearnworlds.com/course/n2kh-advocacy [accessed 03 July 2026].

Government Security Group (GSG), 2026. *Secure by Design Principles*. London: UK Government. Available at: https://web.archive.org/web/20260708103842/https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/

International Labour Organization (ILO), 2022. *Psychosocial risks and Mental Health at Work.* Geneva: ILO. Available at: https://web.archive.org/web/20260708103933/https://www.ilo.org/topics-and-sectors/safety-and-health-work/psychosocial-risks-and-mental-health-work

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC), 2013. *ISO/IEC 27001: Information Security Management Systems – Requirements*. Geneva: ISO/IEC.

Library of Congress, 2026. 'Designing Storage Architectures for Digital Collections'. LOC: Washington DC. Available at: https://web.archive.org/web/20260624204656/https://digitalpreservation.gov/meetings/storage26.html

OECD, 2021. *The OECD Framework for digital talent and skills in the public sector*. Available at: https://web.archive.org/web/20260619103337/https://www.oecd.org/en/publications/the-oecd-framework-for-digital-talent-and-skills-in-the-public-sector_4e7c3f58-en.html

National Digital Stewardship Alliance (NDSA), 2026. *Levels of Digital Preservation*. Alexandria: NDSA. Available at: https://web.archive.org/web/20260708104326/https://www.ndsa.org/publications/levels-of-digital-preservation/

National Cyber Security Centre (NCSC), 2023. *Cloud Security Principles*. London: NCSC. Available at: https://web.archive.org/web/20260703220449/https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

NCSC, 2026. *Cyber Essentials*. London: NCSC. Available at: https://web.archive.org/web/20260702151005/https://www.ncsc.gov.uk/cyberessentials/overview

NCSC, 2025. *Cyber Governance for Boards.* NCSC: London. Available at: https://web.archive.org/web/20260620062537/https://www.ncsc.gov.uk/cyber-governance-for-boards/overview

NCSC, 2026. *Zero Trust.* NCSC: London. Available at: https://web.archive.org/web/20260330173731/https://www.ncsc.gov.uk/collection/zero-trust

National Institute of Standards and Technology (NIST), 2018; updated 2024. *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework, CSF)*. Gaithersburg: NIST. Available at: https://web.archive.org/web/20260707221539/https://www.nist.gov/cyberframework

NIST, 2020. *Zero Trust Architecture (Special Publication 800-207)*. Gaithersburg: NIST. Available at: https://web.archive.org/web/20260708104556/https://csrc.nist.gov/pubs/sp/800/207/final

NIST, 2026. 'least privilege', from the NIST Computer Security Resource Center. Gaithersburg: NIST. Available at: https://web.archive.org/web/20260703222822/https://csrc.nist.gov/glossary/term/least_privilege

Pennock, M., 2023. *A How-To Guide for the CHARM Digital Preservation Risk Reference Model*. University of Dundee. Available at: https://web.archive.org/web/20260708104759/https://discovery.dundee.ac.uk/ws/portalfiles/portal/118440768/02-CHARM_HowToGuide.pdf

Prater, S., 2018. 'How to Talk to IT about Digital Preservation*', Journal of Archival Organization, 14(1–2), 90–101.*Available at: https://doi.org/10.1080/15332748.2018.1528827 [accessed 03 July 2026].

The National Archives (TNA), 2021. *DiAGRAM - The Digital Archiving Graphical Risk Assessment Model*. London: TNA. Available at: https://web.archive.org/web/20260708105209/https://diagram.nationalarchives.gov.uk/