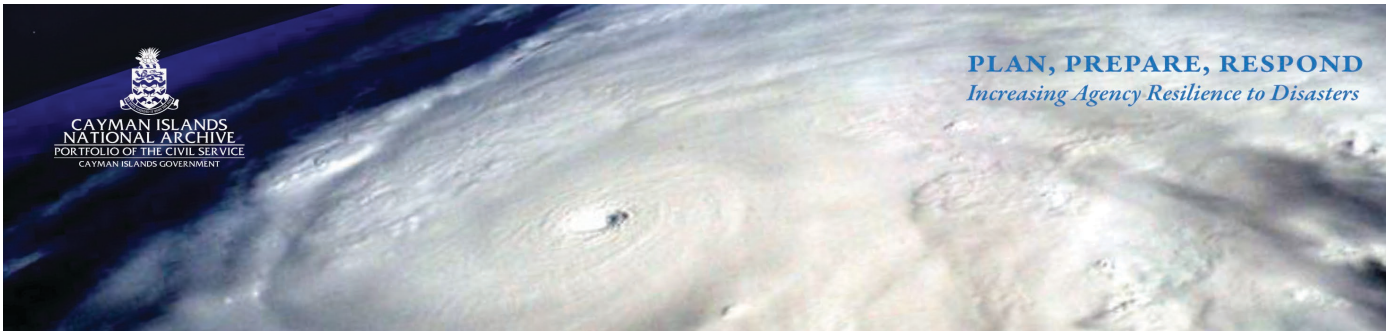

JULY 2025

Securing Continuity with RIM

INSIDE THIS ISSUE:

Records and Information Management (RIM) Amid Administrative Reshuffling

The recent CIG organisational reshuffling has brought significant administrative changes, impacting how records are managed, maintained, and protected. As roles and responsibilities shift, it is critical that all staff clearly understand their duties related to RIM, which ensures compliance with the National Archive and Public Records Act (2015 Revision). This clarity is vital for business continuity, especially in preparing for natural and manmade disasters that may threaten the integrity and accessibility of our public records. Following are some key actions which will help address RIM during administrative changes.

- **Clarify and Communicate Updated Roles:** Inform all personnel of their responsibilities regarding records custody, protection, and recovery.
- **Review and Update Records Surveys/File Plans:** Departments should immediately assess and update their records surveys to reflect changes in custodianship and storage locations.
- **Strengthen Backup and Storage Protocols:** Verify digital backups are current and securely stored off-site or in CLOUD environments. Physical records should be secured in disaster-resistant locations.
- **Update Disaster Recovery Plans:** Align recovery plans with the new organisational structure, emphasising records storage and retrieval procedures.
- **Staff Training:** Ensure staff have a foundational understanding of RIM best practices emergency protocols, allowing for readiness across all teams. See CINA's Introduction to RIM training on CSC Online.
- **Review Access Controls:** Adjust access permissions to reflect new roles, maintaining the security of sensitive records.
- **Document Process Changes:** Action procedural updates related to RIM post-reshuffle to support accountability and smooth transitions.

Business Continuity through Digital Transformation

Section 10 of the *Disaster Preparedness and Hazard Management Act (2019 Revision)* provides the legal basis for the completion of **Business Continuity Plans (BCPs)** in the Cayman Islands. In 2024, Hazard Management Cayman Islands (HMCI) implemented a new software – *Continuity2Meridian* (also referred to as 'Continuity2' or C2) – to manage the process of business continuity planning for the Cayman Islands Government (CIG). With the world becoming increasingly complex and uncertain, the disruptions we face are becoming increasingly unpredictable, therefore traditional approaches to business continuity planning have evolved to enhance organisational resilience.

The C2 platform seeks to strengthen operational resilience in CIG by automating and streamlining plans for the continued delivery of critical government functions and services during and after disruptive events. The Cayman Islands Government has leveraged the *Continuity2Meridian* software to eliminate the current practice requiring manually prepared written plans, and instead, the software automatically generates departmental business continuity plans uniformly across the Cayman Islands public service. Furthermore, this system also highlights the interdependencies between departments and both internal and external suppliers, thereby highlighting potential points of failure in current plans. According to HMCI, "these plans can then be managed, exercised, and tested individually or across government, significantly increasing our resiliency."

Vital Records?

Vital records (also referred to as essential records) are those active records which are essential for the continuation or reconstruction of the operations of your agency in the event of a disaster. They are usually the records which will establish the legal and financial position of the Government, and those critical to the establishment of the rights of the Government, its employees and citizens. When identifying Vital Records, these records typically fall into two categories:

- *Emergency Operational Records* - required for business continuity purposes, i.e. to continue functioning after a disaster; and
- *Legal and Financial Rights Records* - needed to protect the legal and financial rights of the Government and the individuals directly affected by its activities, e.g. its internal and external clients.

It is recommended that agencies maintain a **list of their vital records**, along with instructions on where, how and who can access the records. More details on developing this listing can be reviewed in our our previous **2024 Disaster Bulletin.**

Agencies need to develop a plan of action to respond to emergencies or disasters that may damage an agency's records and to provide for the **recovery of needed information, regardless of the medium of the records**. For example, should the national electricity grid fail, these vital records still need to be accessible. These precursory measures should collectively form part of your Business Continuity Plan (BCP).

Protecting records is critical in an emergency, second only in priority to protecting people. Desks, chairs and tables can be replaced, however people, and the records and information they rely on to carry out their duties – cannot.

Top

Protecting Your Paper Records

The following steps should assist you with protecting your paper records:

- List vital records, identifying locations on floor plans.
- List items in order of priority once vital records have been identified.
- List records before transferring them to off-site storage.
- Store records inside document boxes or fire proof file cabinets.
- Never leave documents out overnight, uncovered.
- Never store records directly on the floor. They should be raised off the floor and stacked no more than three (3) boxes high. Do not store near windows.

- Avoid storing records on the top shelves.
- Pack files vertically, spine down in archival boxes. Do not lay flat or pack box too tightly; leave 1” of space.
- Ensure boxes are secure and tightly sealed; wrap with polythene/plastic sheeting.
- Ensure fire precautions including making staff aware of hazards, appropriate fire preventions and fire fighting tools.
- Keep all aisles, passageways, and exit doors unobstructed.

Top

Notification of Damaged Physical Records

The National Archive's *Guideline 12 Notification of Damaged Records* establishes a mandatory framework for public agencies to notify CINA of any substantial damage, from natural or manmade disasters, to physical (paper) public records. Records created, received and managed by public agencies are considered information assets of the C.I. Government, and should be monitored for accountability and good governance. They provide valuable evidence of business operations to agency clients, as well as legal and strategic planning decisions.

Public agencies should continuously monitor storage areas to ensure records are accessible for as long as they are required. There may be instances where unexpected disasters occur, and protective measures for records should also be incorporated within each public agency's Business Continuity Plan (BCP).

It is essential that agencies document substantial damage to any paper records as a means to either undertake remediation measures, or to ultimately pursue the authorised destruction of records which cannot be recovered (as per CINA's destruction protocols).

Once the damage has been discovered, time is of the essence to stabilise or prevent further issues. Notification of damage should be submitted immediately in writing to the National Archive, along with images and additional evidentiary documentation, using the *Damaged Physical Records Notification Form*.

Agencies should permanently retain a copy of the *Damaged Physical Records Notification Form* for their official recordkeeping system. If damage has occurred as result of a major natural disaster such as a hurricane, the National Archive can also be notified through the procedures of the NEOC.

WHAT IF: CONTINGENCY MANAGEMENT

In planning for natural disaster, one has to assess the risk while balancing the pressures of business continuity. Risk assessment is part of your BCP, for which, agencies should consider the following scenarios:

- *Backup generators fail and there is no electricity to access backups.*
- *Staff are dealing with damage to their own property and are unable to assist with recovery.*
- *Internet and phone providers are down; no access to CLOUD storage.*
- *No means of transportation for staff.*
- *Office building is structurally damaged.*
- *Roads impassable/physically infrastructure heavily damaged.*
- *Keep a copy of relevant contacts readily available.*

Consult CINA Guideline 12 for more information.

Top

Stabilisation and Recovery of Electronic Records

In the event that a disaster affects your facility, consult with first responders. Do not enter your facility until you have received permission to do so, as serious electrical, chemical, and other hazards may be present even in areas that look perfectly safe. If first responders advise destroying your damaged electronic or paper records, assure them that you must first contact the National Archive and your IT service providers, who may have information on how to salvage these materials.

Once you have gained access to your facility, you can begin salvaging electronic storage media affected by the disaster. Begin work as quickly as you can, as the sooner you start salvaging your media, the greater your chances of recovering data. Ideally, your salvage efforts should begin no later than forty-eight hours after the disaster. However, if you are barred from accessing your facility for a week or more, some of your data might still be recoverable.

Preparedness Steps

To mitigate damage to electronic media from disasters, non-technical individuals can take several preparedness steps. These steps focus on prevention, protection, and planning to minimize the risk and impact of potential disasters:

1. Backup Your Data

- **Regular Backups**: Regularly backup important data to multiple locations. Use external hard drives.
- **Automate Backups**: Confirm with CSD that automatic backups are enabled for your business entity and verify the frequency at which they occur.

2. Use Protective Storage

- **Waterproof and Fireproof Containers**: Store electronic media (e.g., external hard drives, USB drives) in waterproof and fireproof safes or containers.
- **Anti-static Bags**: Use anti-static bags for storing sensitive media to protect against static electricity.

3. Proper Environment

- **Climate Control**: Keep media in a climate-controlled environment to avoid damage from humidity and temperature fluctuations.
- **Avoid Direct Sunlight**: Store electronic media away from direct sunlight and sources of heat.

4. Safe Placement

- **Elevated Storage**: Store media on high shelves or in elevated areas to protect against flooding.
- **Secure Locations**: Store media in a secure secondary location that is not susceptible to the same risks or disasters as the primary site. Place media away from potential hazards, such as windows and heavy objects that might fall.

5. Surge Protection

- **Surge Protectors**: Use surge protectors for all electronic devices to protect against electrical surges caused by storms or power outages.
- **Uninterruptible Power Supplies (UPS)**: Install UPS systems for computers to provide temporary power during outages and allow for safe shutdowns.
- **Unplug During Storms**: Unplug electronic devices during severe storms to prevent damage from power surges.

Top

6. Regular Maintenance and Checks

- **Check Backups**: Regularly check that backups are functioning correctly and that data can be restored.
- **Update Software**: Keep backup software and systems updated to protect against vulnerabilities and ensure compatibility.

7. Business Continuity Plan

- **Create a Plan**: Develop your agency's **business continuity plan** outlining steps to take in case of an emergency.
- **Emergency Contacts**: Keep a list of emergency contacts, including professional data recovery services, readily available.
- **Practice Drills**: Conduct occasional drills to ensure everyone knows how to safely secure and handle electronic media during a disaster.

9. Education and Training

- **Learn Basic Techniques**: Learn basic techniques for handling and protecting electronic media.
- **Stay Informed**: Keep informed about common risks in your area, such as floods, earthquakes, or storms, and prepare accordingly.

By implementing these preparedness steps, individuals can significantly reduce the risk of damage to their electronic media from disasters. Regular backups, proper storage, and a well thought-out business continuity plan are crucial components of effective disaster preparedness.

General Guidelines

1. **Safety First**: Ensure your safety by wearing gloves and a mask if necessary, and ensure the area is free from hazards like water or fire.
2. **Do Not Power On**: Never try to turn on or use damaged electronic devices.
3. **Handle with Care**: Always handle damaged media gently to avoid further physical damage.

Steps for Different Types of Damage

Water-Damaged Media

1. **Immediate Action**: Carefully remove the device from the water.
2. **Do Not Shake or Disassemble**: Avoid shaking the device or trying to open it.
3. **Drying:**
    - **Air Drying**: Place the device in a cool, dry place with good air circulation. Do not use a hairdryer or apply direct heat.
    - **Use Desiccants**: Put the device in a sealed container with silica gel packets or uncooked rice to absorb moisture. Leave it for at least 24-48 hours.
4. **Professional Help**: Contact a professional data recovery service as soon as possible.

Top

Fire-Damaged Media

1. **Cool Down**: Allow the device to cool to room temperature naturally. Do not attempt to speed up the cooling process.
2. **Remove Soot Gently**: Use a soft brush or canned air to gently remove any soot or ash. Do not use liquids or abrasive materials.
3. **Professional Assessment**: Do not try to power on the device. Instead, contact a professional data recovery service for further advice and assistance.

Physically Damaged Media

1. **Avoid Further Handling**: Handle the device as little as possible to prevent additional damage.
2. **Use Protective Storage**: Place the device in an anti-static bag or wrap it in a clean, dry cloth.
3. **Contact Professionals**: Seek professional help immediately for assessment and potential data recovery.

Environmental Damage (Mold, Dust)

1. **Clean Gently**: Use a soft, dry cloth or a soft brush to gently remove dust. For mould, do not attempt to clean it yourself; consult a professional.
2. **Dry Environment**: Store the device in a dry, cool environment to prevent further mould growth or dust accumulation.
3. **Seek Professional Help**: Contact a data recovery service if the device has significant mould damage.

Additional Tips

- **Document Everything**: Keep a record of the condition of the media, any immediate actions you took, and contact information for data recovery services.
- **Emergency Kit**: Consider having an emergency kit with basic supplies like anti-static bags, silica gel packets, and a list of professional data recovery contacts.

When to Contact Professionals

- **Complex Damage**: If the damage is extensive or beyond basic drying and cleaning, contact a professional data recovery service.
- **Data Importance**: For critical data, it's best to seek professional help immediately to maximize the chances of successful recovery.

By following these steps, individuals can stablise damaged electronic media and prevent further deterioration. The key is to handle the media carefully, avoid any actions that could worsen the damage, and seek professional help promptly.

Top

Legislative Compliance

Under section 6(2) of the *National Archive and Public Records Act (2015 Revision)*, the most senior officer in public agencies is required to ensure records are maintained in good order and condition. Additionally, the National Archive's *Creation and Maintenance Standard (S1)* sets out the minimum recordkeeping measures. The quick self-assessment tool below should help agencies evaluate themselves against the preservation metrics listed in the *Standard*. In undertaking this assessment, it is best to be as candid as possible in order to identify any deficiencies, and then work on increasing compliance, as and if necessary. Should agencies have any concerns or questions they can contact the National Archive at cina@gov.ky.

S1 section	Requirements S1	Questions	Response	Suggested Remedial Response
7	**Temperature, RH and Light:** Records can deteriorate if exposed to too much light, particularly sunlight. They should be stored in stable environmental conditions; temp 60° – 80° F and RH 30 – 60%.	Are records subjected to direct sunlight? Are temperatures and relative humidity within acceptable ranges?	□ Yes □ No □ N/A □ Unsure	• Move records away from direct sunlight. • Check and maintain air-conditioning systems. • Consider using a humidifier.
8(2)	**Pests – insects and vermin:** Silverfish and mice can do considerable damage; infestation may spread when records are moved around.	Are there signs of rodents, silverfish or other pests?	□ Yes □ No □ N/A □ Unsure	• Regular inspection of records for signs of deterioration/degradation from pest and mould must be carried out.
8(2)	**Mould:** Mould will usually affect areas with high humidity and/or without air circulation. Mould is a health risk for staff and can damage records.	Is the location damp or mouldy? Is there growth on papers?	□ Yes □ No □ N/A □ Unsure	• If mould is identified in your storage area, move unaffected records to a new location. • If records are already affected by mould, contact the Department of Environmental Health for an assessment, and the National Archive for further advice.
8	**Storage:** Storing records on the floor puts them at risk of flooding or water build-up. It is also a safety issue for staff.	Are records stored on the floor?	□ Yes □ No □ N/A □ Unsure	• Use storage cabinets and/or shelving units. • Standards for records storage recommend a height of 4 inches off the floor. • Do not stack more than 4 boxes on each other as the lower ones may crush under the heavy weight.
7(5) 8	**Security of the location:** Records should not be kept in areas that are accessible by unauthorised persons.	Is the location accessible by unauthorised persons, and is it protected from potential theft?	□ Yes □ No □ N/A □ Unsure	• Identify who has access to your storage areas, ensuring the areas are properly secured and monitored. • Limit access to storerooms to authorised staff only, or, if not possible, keep records in locked cabinets.
8	**Fire and water:** Storage facilities are to be protected from fire and water hazards.	Are records near water pipes, sinks, toilets; are there any signs of leaks? Are records near electrical outlets?	□ Yes □ No □ N/A □ Unsure	• Consider relocating records. • Repair or discontinue use of electrical outlets. • Install smoke/fire detection systems, including fire extinguishers. • Inspect storage areas regularly.
7(3) 8(1)	**Dedicated record storage areas:** Eating, drinking, and smoking must not be permitted in storage areas.	Is there evidence of eating and drinking in record storage areas?	□ Yes □ No □ N/A □ Unsure	• Clean area and ensure that all staff are aware that no food or drinks should be consumed or even stored in these areas.

Top

Checklist for Business Continuity Plans

☐ **Risk assessment** - Identify potential risks and their effect on records and information management systems, and then outline the mediation steps and monitoring processes.
- If a disaster occurred, how long could the agency function with available staff until records and recordkeeping systems are back online?

☐ **Pre-disaster planning** - In your plan, outline the duties/tasks of those responsible for records disaster mitigation and have specific recovery/remediation procedures for dealing with the identified disasters.
- Has adequate storage and security of the records been identified?

☐ **Communication** - Identify who should be informed in the event of a records disaster and how information will be exchanged. Include instructions on the means of interacting with your stakeholders (e.g. staff, clients and vendors).
- Has your agency's team been briefed? Plan the recovery approach and assign tasks.

☐ **Disaster co-ordination** - Compile a contact list of external emergency service agencies including the National Archive, the Department of Environmental Health, NEOC, and Hazard Management Cayman Islands.
- Identify the external services/vendors required for normal business operations.

☐ **Disaster response** - Activate the plan, with priority given to the recovery of vital records and critical data (including lists of records and their locations). Procedures should be in place for handling damaged materials, including the required resources (e.g. staff, alternate locations, equipment, etc.).
- Secure affected areas and assess any damage to records, particularly vital records. Endeavour to collect evidence of damage as quickly as possible with photos and/or written notes/reports. Submit all documentation, along with a *Damaged Physical Records Notification Form* to the National Archive.

☐ **Recovery** - Undertake and coordinate the activities for record recovery/remediation, and establish procedures for handling records after a disaster.
- Do not dispose of damaged records as they may be salvageable; consult with the National Archive.

No public records can be destroyed without an approved disposal schedule and in accordance with the National Archive's documented destruction process.

☐ **Post recovery** - Review and update the plan.
- What worked and what can be improved.