AUDITOR GENERAL'S DEPARTMENT OF JAMAICA

HURRICANE MELISSA RELIEF INITIATIVE AUDIT

SUPPORT JAMAICA WEBSITE

Information Technology Audit Report

February 2026

"A better Country through effective audit scrutiny"

Background

1

Supportjamaica.gov.jm website donated by a private developer to mobilise donations, track emergencies, and coordinate recovery efforts in the aftermath of the hurricane.

2

On October 28, 2025, Hurricane Melissa struck Jamaica, resulting in extensive destruction and immediate humanitarian concerns

3

Melissa relief initiatives, including an assessment of the website's information security controls, commissioned on 2025 November 5.

Background *(cont'd)*

Deed of Agreement executed on 2025 December 27 between ODPEM and the private developer to formally record and establish the mutual understanding, intentions, and commitments with respect to the development, donation, and continued use of the website.

Audit report prepared on user access management and data protection measures in place up to 2026 January 20.

Audit Overview

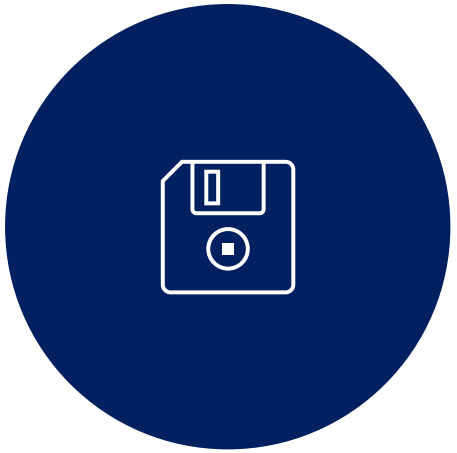
Key Audit Question

Did appropriate IT controls exist over the *supportjamaica.gov.jm* website to ensure information security?

What We Found:

User Access Management

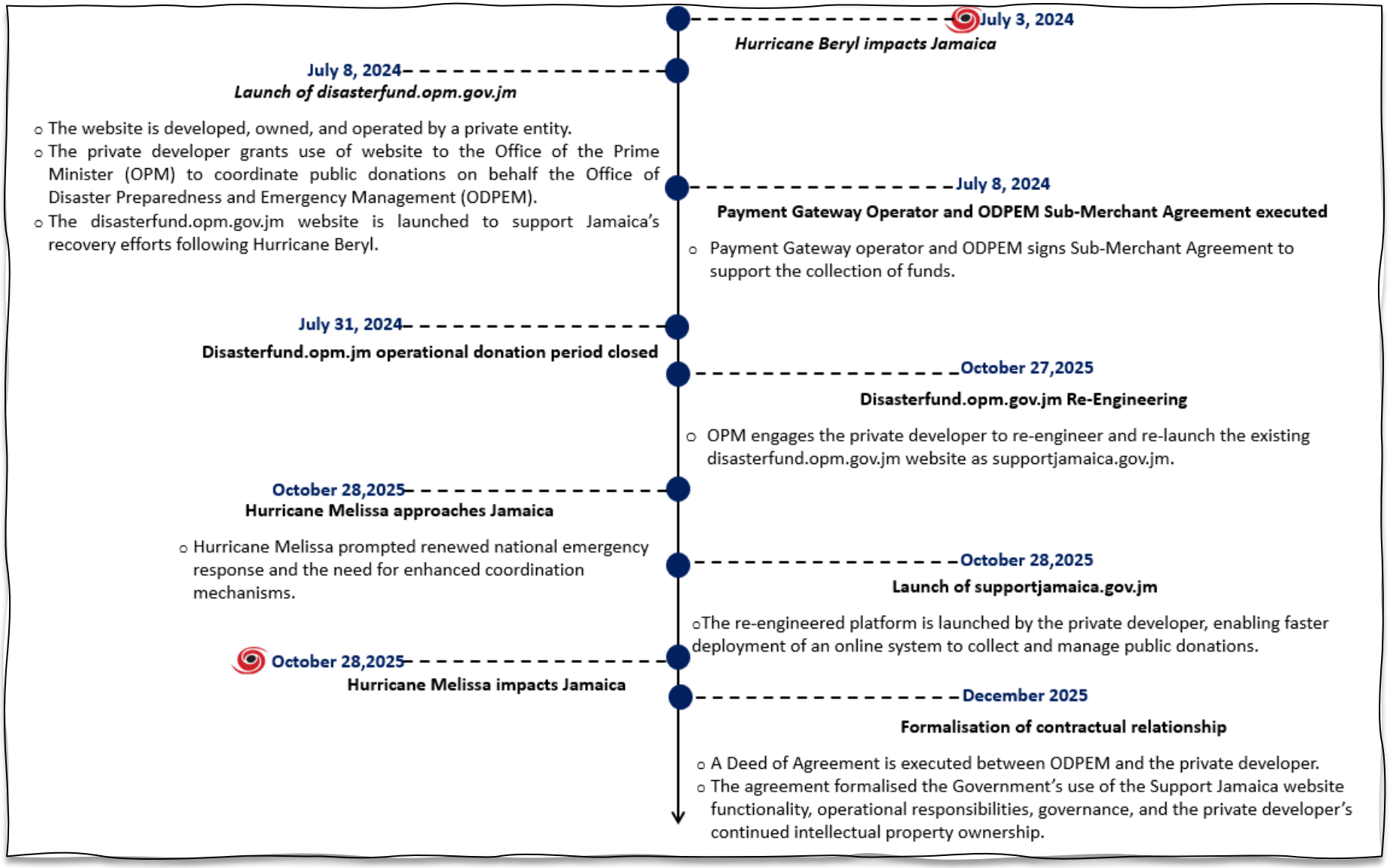
Weak controls over user permissions and system access



Data Protection Non-Compliance

Failure to comply with data protection laws and agreement

Support Jamaica Website Timeline



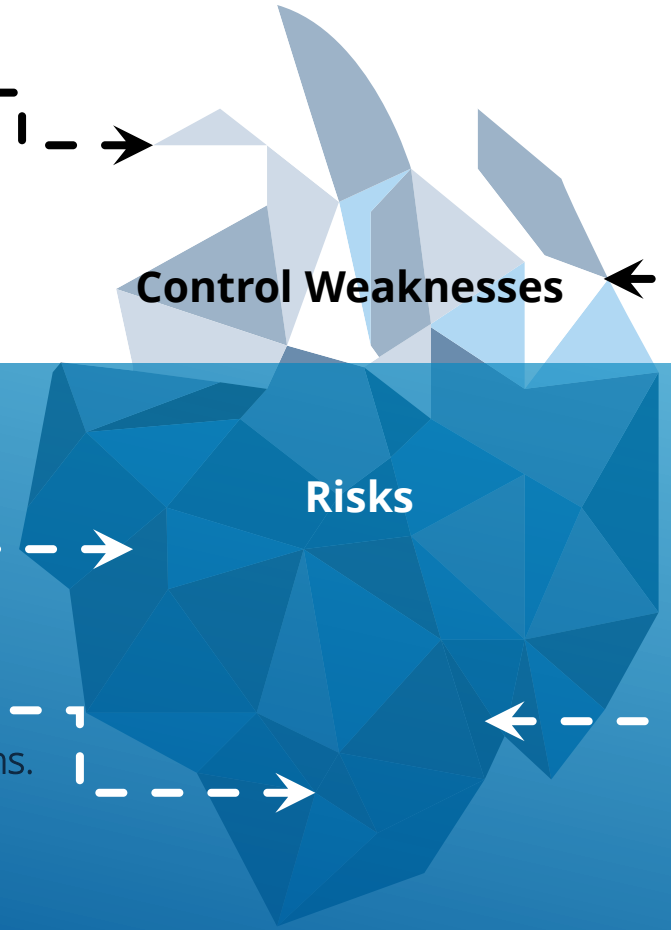
Information Security (IS) Governance Gaps

Draft Security Policies

ODPEM lacked formally approved Information Security and Access Control policies for managing user access.

Absent Access Control Framework

ODPEM lacked an enforceable user account management standard for the Support Jamaica–Administrative dashboard.



Inappropriate/Unauthorised Access

Users granted access to data and systems without proper justification.

Weakened IS Management System

Roles, responsibilities, and access control principles were not clearly defined or communicated.

Inconsistent Security Practices

Ad hoc assignment of user rights and permissions.

Inadequate User Access Management

We identified gaps in user access management, including insufficient controls over access permissions, deprovisioning and the monitoring of accounts.

An external user was elevated to the "Super Admin" role and subsequently provisioned multiple accounts without a documented basis for the level or duration of access granted.

Elevated

Undocumented

Access was granted to eight external officers without documented requests, approvals, or evidence that the permissions assigned aligned with their official roles and responsibilities.

Inadequate User Access Management

The audit confirmed the deprovisioning of only two external officers, as the relevant audit log evidence was unavailable for the other six accounts.

Incomplete

Misaligned

The Head of the Entity was assigned the “Super Admin” role by an external user that provides full administrative, operational, reporting, and security privileges though system administration responsibilities were not consistent with his job function or justified.

Inadequate User Access Management *(cont'd)*

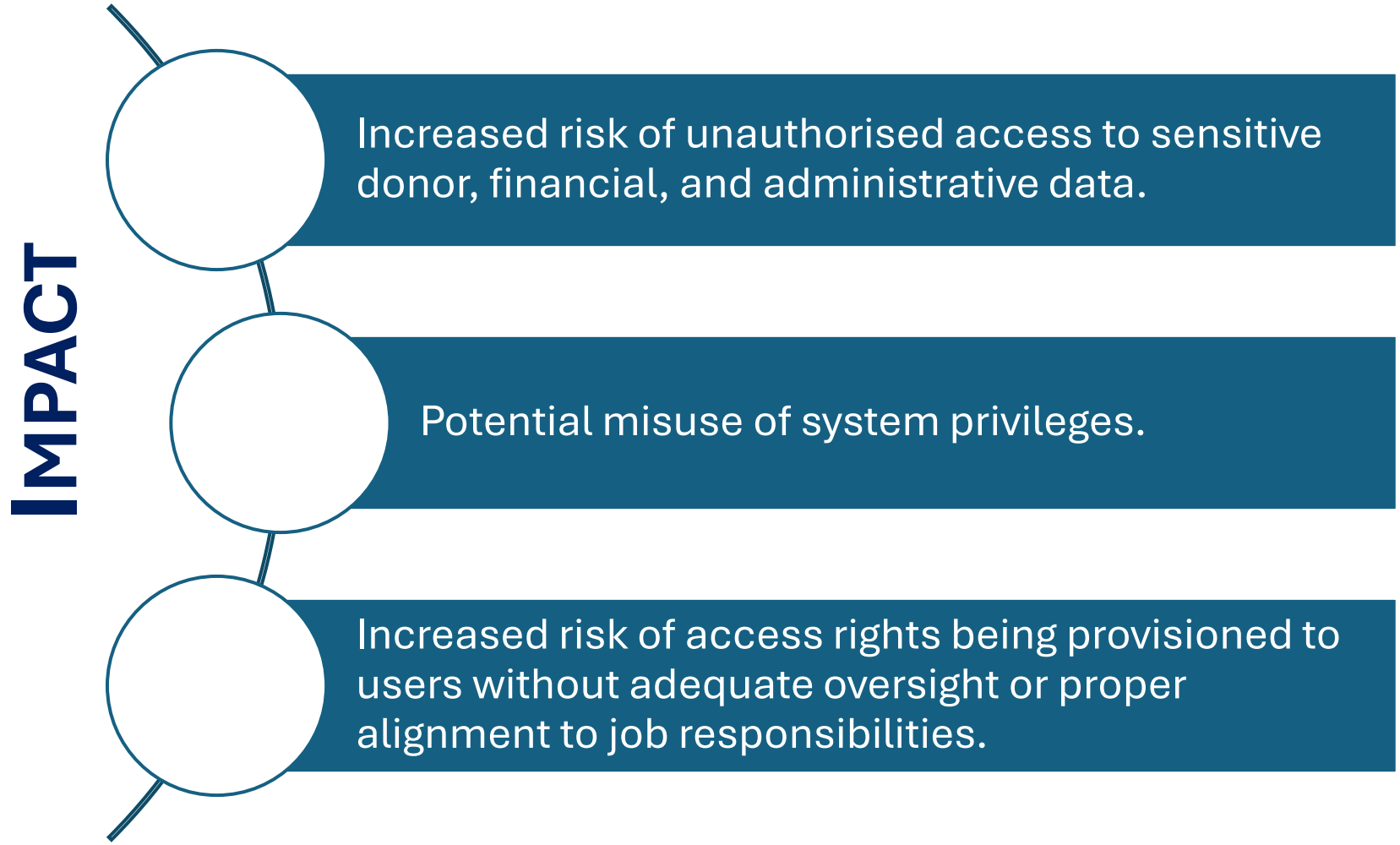
Absence of Segregation of Duties

ODPEM did not effectively separate the roles of requesting, approving and implementing access to the Support Jamaica – Administrative Dashboard.

Privileged Accounts Insufficiently Managed

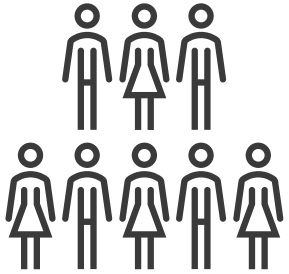
- Records for privileged access and changes were not maintained.
- Privileged access accounts were not monitored.

Inadequate User Access Management



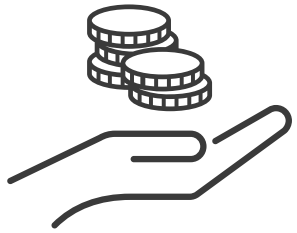
Non-Compliance with Data Protection Act (DPA)

Since its launch, the Support Jamaica website has facilitated donations from individuals and supported community engagement. The website also collects personal information from donors and volunteers, highlighting the need for strong data protection controls.



16,900

donors



US$1,399,262
JM$71,358,183

in funds collected as at 2026 January 11

4,698

volunteers registered between 2025 November 1 and 2026 January 19

AUDITOR GENERAL'S DEPARTMENT OF JAMAICA

Non-Compliance with Data Protection Act (DPA) *(cont'd)*

We found significant shortcomings in data protection controls and statutory compliance.

Security Measures Unverified

Data Processing Agreement signed with private developer, but ODPEM did not independently confirm the implementation of the specified security measures.

Non-Compliant Developer

Data Processing Agreement indicates compliance with SOC 2 Trust Services Criteria*, but the private developer was not compliant up to 2026 January 20.

Access Undisclosed

The Support Jamaica website's Privacy Policy failed to disclose the developer's access to personal data.

**SOC 2 (System and Organisation Controls) Trust Services Criteria (TSC) are a set of standards established by the American Institute of Certified Public Accountants (AICPA) to evaluate how organisations manage and protect customer data. The five criteria are Security (mandatory), Availability, Processing Integrity, Confidentiality, and Privacy.*

Non-Compliance with Data Protection Act (DPA) *(cont'd)*

DPO Unassigned

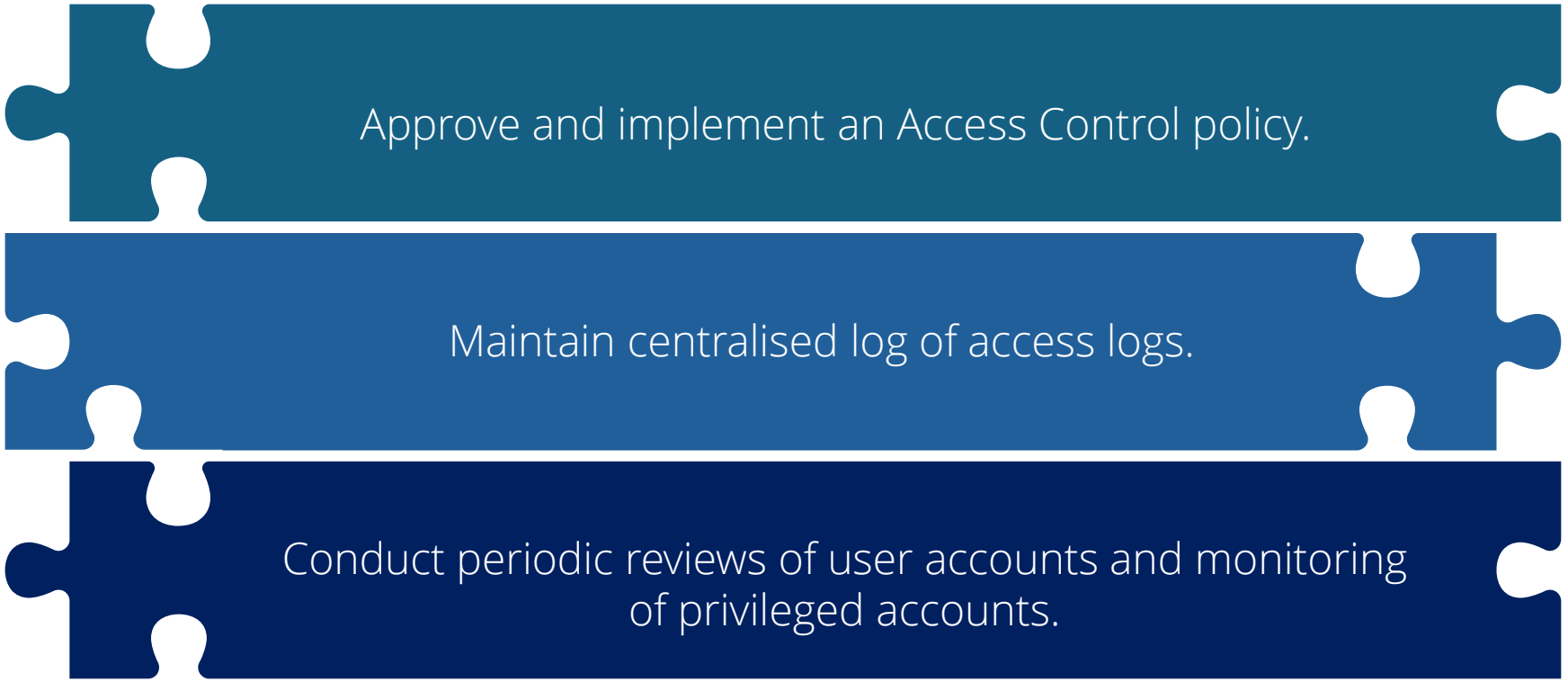
The Privacy Policy refers to a Data Protection Officer (DPO), but ODPEM had not appointed an officer with these responsibilities.

DPA Gaps

ODPEM breached Section 15 of the DPA, which prohibits the processing of personal data without an organisation being registered.

User Access Recommendations

To ensure appropriate user access and system governance on the supportjamaica.gov.jm website, the following access control recommendations should be implemented in accordance with industry best practices.



Data Protection Recommendations

To maintain secure and responsible operations on the supportjamaica.gov.jm website, it is important to implement the following recommendations related to data protection, in keeping with industry best practices.