GENERAL INFORMATION TECHNOLOGY AUDIT

OF

SUPREME AND MAGISTRATE'S COURTS
JUDICIAL ENFORCEMENT MANAGEMENT SYSTEM
CASE MANAGEMENT SOFTWARE

2001 – 2019

Office of the Auditor General

September 2020

TABLE OF CONTENTS

ABBREVIATIONS

DITES	Department of Information Technology and e-Services
ECSC	Eastern Caribbean Supreme Court
GoM	Government of Montserrat
IS	Information Security
ISAE	International Standard on Assurance Engagements
ISSAI	International Standard of Supreme Audit Institutions
IT	Information Technology
JEMS	Judicial Enforcement Management System
LAN	Local Area Network
OAG	Office of the Auditor General
ODG	Office of the Deputy Governor
OECS	Organisation of Eastern Caribbean States
PCSS	Professional Computer Software Services
PDF	Portable Document Format
PWD	Public Works Department
SA	System Administrator
SLA	Service Level Agreement
SQL	Structured Query Language
UPS	Uninterruptible Power Supply
USAID	United States Agency for International Development
VA	Volt-ampere
VPN	Virtual Private Network

PREAMBLE

Vision Statement

To be a proactive Supreme Audit Institution that helps the nation make good use of its resources

Mission Statement

The O.A.G is the national authority on public sector auditing issues and is focused on assessing performance and promoting accountability, transparency and improved stewardship in managing public resources by conducting independent and objective reviews of the accounts and operations of central government and statutory agencies; providing advice; and submitting timely Reports to Accounting Officers and the Legislative Assembly

The Goal

To promote staff development, enhance productivity, and maintain a high standard of auditing and accounting in the public sector, thereby contributing to the general efficiency and effectiveness of public finance management


OFFICE OF THE AUDITOR GENERAL
MONTSERRAT

AUDITOR GENERAL'S OVERVIEW

We conducted a General IT Audit of the Judicial Enforcement Management System (JEMS) software. Overall, we sought to establish if JEMS enabled the Montserrat branches of the Supreme and Magisterial Courts to meet their mandates and business goals through measures and controls in the areas of IT Governance, IT Operations, Business Continuity and Disaster Recovery, Information Security, and Application Controls.

The review revealed that the JEMS software is robust, and has adequate and very effective provisioning in place to ensure sensitive judicial information inputted into the software, is accurate, valid, and safeguarded from unauthorised access, and copying or viewing. However, the version used in Montserrat is very outdated and we identified quite a few Information Security vulnerabilities at both courts.

We have highlighted other findings and provided a number of recommendations that we feel would benefit the Judicial Courts, once they are implemented.

Subsequent to our audit, we noted that due to the COVID-19 pandemic both judicial departments have either resolved or implemented solutions to existing issues identified during the course of this review.

We wish to thank the Montserrat Supreme and Magisterial Courts staff and all other persons who provided information, clarifications, or extended courtesies to the auditors during the course of this review.

Florence Lee
Auditor General
9 December 2020

EXECUTIVE SUMMARY

Overview

1. The Judicial Enforcement Management System (JEMS) is a case management package software that gathers and provides the Eastern Caribbean Supreme Court (ECSC) in St Lucia, with statistical information from all of the Organisation of Eastern Caribbean States member states courts. The application was launched in the ECSC in 2000, and in the ECSC Member State country of Montserrat, in October 2001.

Key Observations and Findings

2. **Adequate software measures and controls in place.** Although outdated, the JEMS software is still very effective with adequate provisioning in place for IT Governance, IT Operations, Business Continuity and Disaster Recovery, Information Security and Application Controls.

3. **Development, Acquisition & Outsourcing.** Development and Acquisition activities were not undertaken by the individual OECS member courts, as the software vendor and the software were solicited and acquired by the ECSC in St Lucia; however, each OECS member court was required to sign a license agreement from the vendor. The ECSC does not own the software or related intellectual property rights; but the ECSC and each Member State country owns the information entered and stored in JEMS.

4. **Change Management initiative.** At the time of the audit, the Montserrat branch of the ECSC, and other Member State countries were in the process of replacing JEMS with the web-based *E-Litigation Portal for Courts* solution. Employees at the Montserrat Supreme Court, Office of the Attorney General, and Department of Public Prosecution, including private sector Lawyers, underwent mandatory training prior to the official launch in March 2020.

5. **Information Security weaknesses.** The audit identified the following vulnerabilities in each judicial department:

   a) <u>Supreme Court Registry & Court Room</u>

   - The Supreme Court Registry office and the Court Room are not outfitted with smoke detectors, fire alarms, or fire extinguishers.
   - The door at the lower level entrance of the Court Room, main, and inner doors of the Court Room are always left unlocked and unmonitored when there is no High Court. This is a very risky practice, as there is the potential for unauthorised individuals to:
     - gain unlawful access to High Court documentation
     - damage or destroy the Court Room and property within
     - conceal weapons or dangerous devices inside the Court Room
     - perpetrate bodily harm to the employees.

b) Magistrate's Court

- The Magistrate's Court office and Court Room are not outfitted with smoke detectors, fire alarms, or fire extinguishers, eight years later after the double arson attack on the Magistrate's and High Courtrooms, on 3rd December, 2012.
- The Executive Officer/JEMS System Administrator's (SA) computer malfunctioned months prior to the audit, and it was temporarily replaced with two temporary computers. One was a laptop with specifications that did not meet the system requirements for the operation of the JEMS software; and the other computer unit malfunctioned. Therefore, the Magistrate's Court JEMS SA was unable to gain access to, and perform administrative tasks in JEMS.

Recommendations

6. **Procurement and installation of fire suppression apparatus.** The absence of early detection devices and warning system, and fire suppression equipment in either of the judicial offices, has the potential to have disastrous outcomes in terms of loss of human life, judicial, and irreplaceable historical information; in particular at the Supreme Court Registry. Therefore, we are strongly recommending that the Supreme and Magistrate's Courts both invest in at least 1 or 2 canisters of either foam and/or powder fire extinguishers.

7. **Implement Physical Access Security protocols.** We strongly recommend that the Supreme Court Registry consider effecting the following protocols for controlling access to the Court Room:
   - Keeping the lower level main front door locked once the High Court is not in session; and only the Supreme Court staff should have access, whenever the department requires documentation.
   - Persons accessing the High Court Reporter should report to the reception area from where the Court Reporter will be alerted. These person(s) are to be either escorted up by Reception, or received by the Court Reporter at the landing.
   - Install a swipe key card system that produces an audit trail of entrance and exit.

8. **Replacement personal computer.** We recommend that the Magistrate's Court continue to liaise with DITES to procure a suitable desktop computer as soon as possible, to enable the JEMS SA to resume oversight of the JEMS application.

Audit Conclusion

9. The Office of the Auditor General has determined that the JEMS 6.0 case management software application has benefited the Montserrat Supreme and Magistrate's Courts; but it is outmoded. It is adequately secure and provides for the input, organisation of data, secure storage, and retrieval of Montserrat's court information.

10. The weaknesses identified were mainly in the areas of Information Security, IT Operations, and Business Continuity and Disaster Recovery. Operational effectiveness and efficiency will be achieved, once the Montserrat judicial departments address the inadequacies and implement the recommendations.

Subsequent Events

11. The investigative aspect of the audit was completed two weeks before the island went on locked down due to the COVID-19 pandemic; as a result, the finalization of the audit report was delayed. Since the re-opening of Government offices in May 2020, the Magistrate's Court JEMS System Administrator received a new computer; purchased a smoke detector for the courtroom; and consulted with Fire and Rescue Services about the acquisition and installation of fire extinguishers for both the main office and courtroom. In addition, the entrance of Supreme Court/Registry building was modified July 2020 to control access into the main office.

CHAPTER 1 INTRODUCTION

Background

1.1 Over the past few years, the Eastern Caribbean Supreme Court (ECSC) has been reviewing and implementing a number of initiatives which are geared towards Judicial Reform in the region. As a result, the Supreme Court formed an Information Technology Committee headed by the Chief Justice to review solutions which would assist with the management of cases filed in the High Courts. After a lengthy and comprehensive process, the Committee selected the Judicial Enforcement Management Systems (JEMS) software package which was developed by the Professional Computer Software Services (PCSS) Inc. The software was designed to enable the High and Appeals Courts to manage court cases from initial filing to final disposition.

1.2 In March 2001, the JEMS software solution was implemented at the Court of Appeal Office at the Eastern Caribbean Supreme Court Headquarters in St. Lucia; and the Montserrat Supreme Court launched JEMS in October, 2001.

Management Responsibility

1.3 Management is responsible for ensuring that appropriate policies and effective controls exist to guide the facilitation of JEMS software. More specifically, management must ensure that policies exist to facilitate IT governance and acquisition of IT products, IT operations, outsourcing, or soliciting of software, information security, business continuity, and disaster recovery. Management is also responsible for establishing appropriate IT controls and for ensuring that they function effectively.

Auditor's Responsibility

1.4 Our responsibility is to independently express a conclusion on the General IT Control audit of the Supreme and Magistrate's Courts JEMS software, based on our audit. Our work was conducted in accordance with International Standards of Supreme Audit Institutions (ISSAI) 100 and International Standard on Assurance Engagements (ISAE) 3000. These principles require that we comply with ethical requirements and plan and perform the audit in order to obtain reasonable assurance whether tried and true policies, plans, procedures, and internal controls exist and are functioning effectively, proper records have been and are being kept, and all the necessary information and explanations for the purpose of our audit, has been obtained.

Audit Mandate

1.5 The Office of the Auditor General (OAG) is mandated through the Montserrat Constitution Order 2010 to perform the audit. This mandate is supported by International Standards of Supreme Audit Institutions (ISSAI) 1, 200, 300, 400, and strengthened by the Public Finance Management and Accountability Act (PFMAA) 2008 and the Public Finance Management and Accountability Regulations (PFMAR) 2009.

Audit Standards and Guidelines

1.6 The standards and guidelines used to assess the JEMS software included the International Standards of Supreme Audit Institutions (ISSAI) 3100, 4100, 5300, and 5310.

Audit Objectives

1.7 The aims of this General IT audit, were to:

(a) Determine if the Supreme and Magistrate's Courts have organisational structures, that enable these legal departments to meet their mandates and business goals; if the judicial staff are sufficiently qualified/trained to use JEMS; and if access to the system is authorised and as per their job function.

(b) Determine whether the Supreme and Magistrate's Courts ensure that the system capacity and performance meets current and future business needs; evaluate the effectiveness of JEMS problem and incident management policies and procedures; and if there are standardised procedures for controlling any changes in JEMS.

(c) Assess how the Supreme and Magistrate's Courts managed the acquisition of JEMS; how these departments ensured JEMS met their quality goals and if either entity has a standardised solicitation plan, or procedure(s).

(d) Assess whether the Supreme and Magistrate's Courts has a Service Level Agreement and/or Contract detailing all its requirements and actively monitors the vendor against the agreement; and takes appropriate action when performance or quality deviates from established baselines; if both Courts' data protection requirements are identified and are a part of the contractual requirements; and if these legal departments retain business knowledge and ownership of JEMS business processes.

(e) Establish if JEMS ensures data integrity, validity, and reliability throughout the processing cycle; that the output information is complete and accurate before further use; if it is properly protected; and that valid data is being entered into JEMS by authorised users only.

(f) Determine if the Supreme and Magistrate's Courts have adequate Physical Access and Environmental Security Controls in place to prevent theft or damage of JEMS-related hardware; unauthorised access to the software; and the unlawful copying or viewing of the JEMS sensitive information.

(g) Determine if the Supreme and Magistrate's Courts have a Business Continuity and/or Disaster Recovery Plan to ensure the security of the JEMS data, software, and hardware.

Audit Scope and Methodology

1.8 The study will cover the period October 2001 - December 2019, and will focus on the examination of the JEMS software. The Auditors will monitor the audit in the field and may amend any area or the audit scope in consultation with the Auditor General, so as to maximise the efficiency of the audit.

1.9 A combination of techniques were utilised to gather information and validate the general controls of JEMS software. These included, but were not limited to, interviewing key personnel from the Supreme Court Registry and the Magistrate's Court who use the

software; inspection of documents; and observation of the software; in order to gather in-depth information about JEMS.

1.10 The findings of this study were discussed with the Registrar, Court Administrator/JEMS System Administrator at the Supreme Court; also the Chief Magistrate, and the Executive Officer/JEMS System Administrator, at the Magistrate's Court. Their comments were taken into consideration when finalising the report.

CHAPTER 2 EASTERN CARIBBEAN SUPREME COURT

2.1 The Eastern Caribbean Supreme Court (ECSC) was formerly known as the West Indies Associated States Supreme Court, which was established by Court Order No. 223 of 1967. This Court Order replaced both the United Kingdom's 1959 Windward and Leeward Islands (Courts) Order in Council and the 1962 British Caribbean Court of Appeal Order in Council.

2.2 The West Indies Associated States Supreme Court had unlimited jurisdiction throughout the newly associated states of the United Kingdom namely Antigua and Barbuda, Dominica, Grenada, Saint Christopher-Nevis-Anguilla, Saint Lucia and Saint Vincent and the Grenadines. This Supreme Court Order also made provisions for the Court to service the remaining British colonies of Montserrat and the Virgin Islands. After Anguilla broke away from St. Kitts and Nevis in 1980, it joined with the other British Territories.

2.3 The Court was retitled the ECSC in 1983 and still is the superior court of record for the Organisation of Eastern Caribbean States (OECS) six (6) independent Member States and the remaining three (3) British Territories. Each Member State and Territory has to furnish the ECSC with an annual contribution to sustain the Court. The functions of the ECSC include:

(i) the interpretation and application of laws of the various member states of the OECS;

(ii) deciding cases of both civil and criminal matters; and

(iii) hearing appeals.

2.4 The organisation consists of a Court of Appeal and a High Court of Justice; the Court of Appeal is itinerant, that is traveling to each Member State and Territory where it sits at various specified dates during the year to hear appeals from the decisions of the High Court and Magistrates Courts in Member States in both civil and criminal matters. Each member state and Territory has its own Court Office, which in addition to the High Court Registry, houses the office of the local High Court judge(s). Filing in the Registries commences the proceedings in matters before the High Court in each of the nine countries and the Court of Appeal. [1,2,3]

Montserrat ECSC Branch

Supreme Court Registry

2.5 **Function**. The Supreme Court Registry office files, records, and manages all Criminal, Civil, Matrimonial, and Probate cases.

2.6 **Mission Statement**. The Supreme Court Registry's mission is to deliver high quality, professional, efficient, and impartial services in facilitating the effective administration and dispensation of justice.

2.7 **Vision Goal**. The vision of the Supreme Court Registry is to be a department which embodies equity and reliability in the administration of Justice.

[1] *https://www.eccourts.org/court-overview/*

[2] *1967 No. 223 ASSOCIATED STATES, The West Indies Associated States Supreme Court Order 1967*

[3] *ECSC 50TH ANNIVERSARY MAGAZINE, CELEBRATING THE PAST, EMBRACING THE FUTURE, pages 08, 09, & 28*

2.8 **Legal Framework.** The Supreme Court Registry is mandated by the *CAP 2.01 Supreme Court Act* and guided by the *ECSC Civil Procedure Rules 2000*.

Magistrate's Court

2.9 **Function.** The Magisterial Department files, records, and manages all Criminal (Summary and Indictal), Civil, Labour, Juvenile, Drug, Quasi (Maintenance and Domestic Violence), Liquor license, Special sittings - Examination of Jurors list, and Traffic cases.

2.10 **Mission Statement.** The Magistrate's Court mission is to efficiently and effectively perform their responsibilities of providing access to an accountable, independent, and impartial system of justice administered according to law.

2.11 **Vision Goals.** The Magistrate's Court is a strong, trusted, independent, and responsive court services that effectively and equitably serve the needs of the community. The entity underpins their vision with the following values:

- Working together as professionals to ensure that the Court delivers outstanding services to the community.
- Behaving ethically and function efficiently in an open, accountable, responsive, and responsible organisation.
- Pursuing excellence by valuing and supporting innovation and initiative. The department also aspires to utilise their resources efficiently and effectively.
- Treating all people equally and with respect by not discriminating; being open-minded and provide the best service they can to individuals; are courteous to each other and the people they interact with; and behave honestly, fairly and with integrity.

2.12 **Legal Framework.** The Magistrate's Court is mandated by the *CAP 2.02 Magistrate's Court Act* and guided by both the *CAP 2.02 Magistrate's Court Rules*, and the *ECSC Civil Procedure Rules 2000*.

CHAPTER 3 IT GOVERNANCE

Organisational Structures

3.1 In both judicial departments, only a select number of staff are authorised to perform JEMS related tasks alongside their routine job duties. The Supreme Court's Administrator and the Magistrate's Court's Executive Officer are the JEMS System Administrators. Two Clerical Officers at the Magistrate's Court, and one from the Supreme Court, double as JEMS Data Entry Clerks.

3.2 All of these select employees are suitably qualified, and have been formally trained, to use the JEMS system either by PCSS Inc., ECSC IT personnel, or received in-house training from the System Administrators. JEMS manuals were disseminated to the users after training for further reference and guidance.

3.3 Over the years, the JEMS System Administrators from both judicial departments continued attending training workshops facilitated by the ECSC, since the software was initially launched in Montserrat in October 2001.

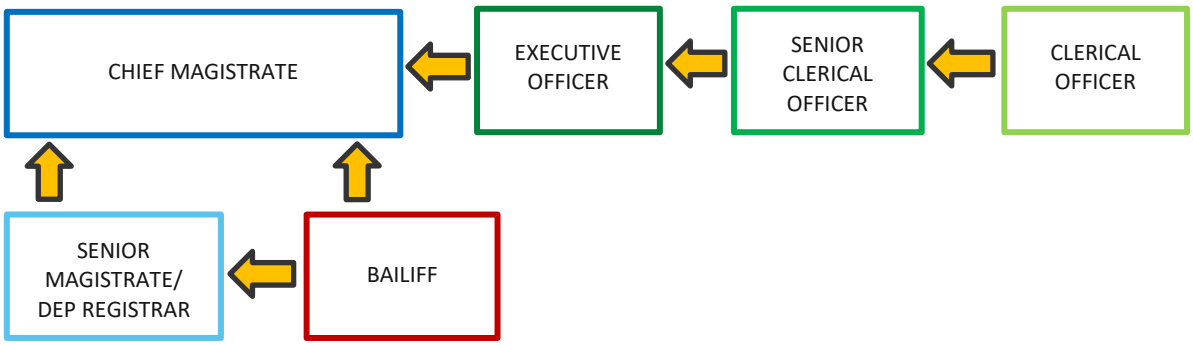


Figure I - Magistrate's Court Organisational Chart

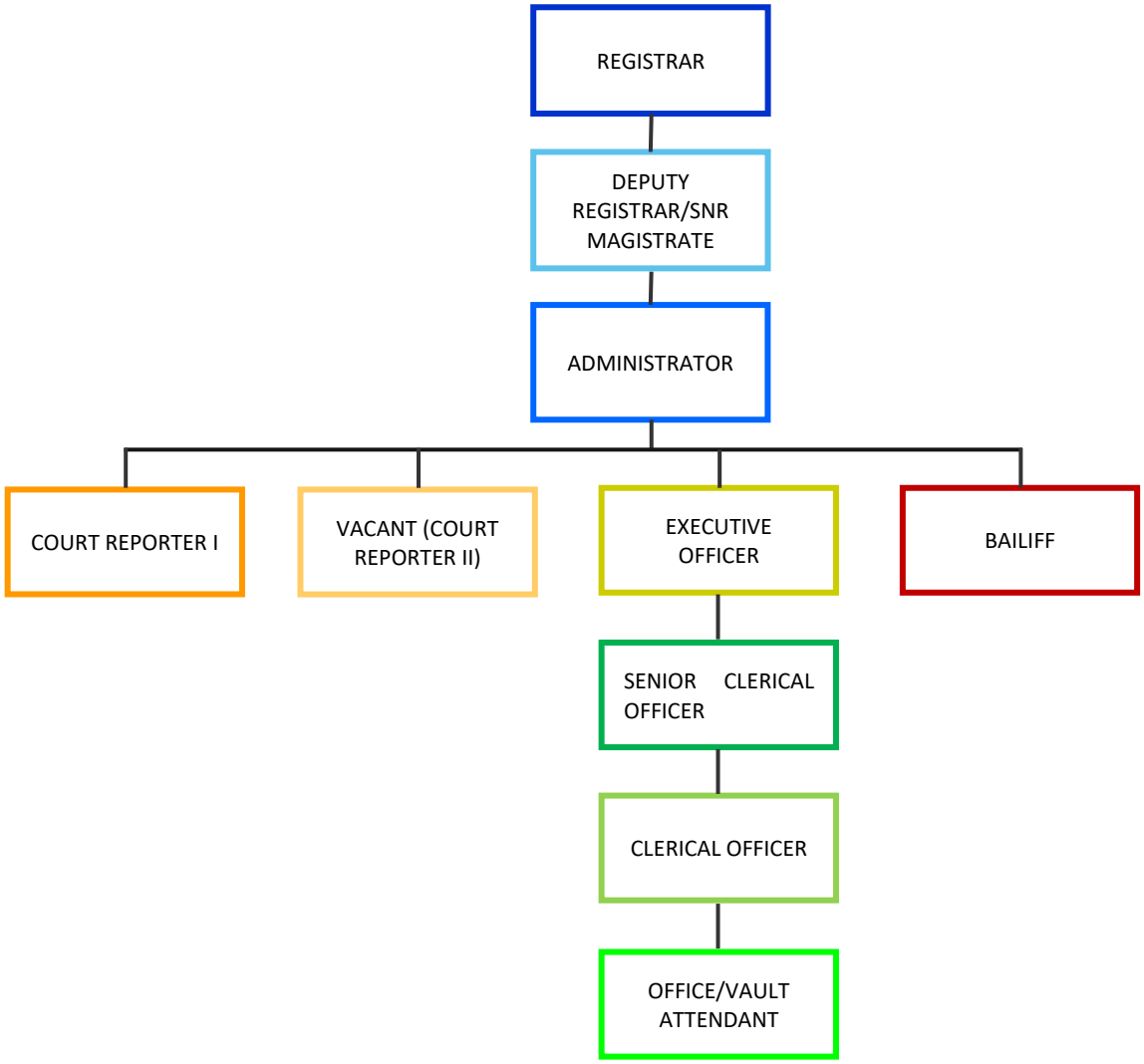


Figure II - Supreme Court Organisational Chart

CHAPTER 4 DEVELOPMENT, ACQUISTION & OUTSOURCING

4.1 **Development, Implementation and Maintenance Costs** [4]The Judicial Enforcement Management System (JEMS) is a Case Management package software that gathers and provides the ECSC in St Lucia, with statistical information from all of the OECS member states courts; the application was developed by the software company Professional Computer Software Services (PCSS) Incorporated, and implemented in the ECSC in 2000. The implementation process commenced with the training of about 40 court office staff from each Member State and Territory over a three week period, where the representatives were trained how to install and operate the JEMS application software. The local governments signed individual Licence and Support Agreements and collectively paid over US$427,000, for the purchase of software licences. The United States Agency for International Development (USAID) provided hardware for the independent Member States; that is, server, workstations, printers, scanners, and Uninterruptible Power Supplies (UPSs).

4.2 The software was definitively launched in 2001 in all of the High Courts of the Member State countries and all cases file since January 2001, were entered into JEMS. Since its implementation, JEMS has afforded all the Courts with the capability to electronically: (i) manage most aspects of court cases, from initiation to deposition; (ii) enter a significant amount of case-related information; and thereby (iii) increasing the ease of access, storage, and retrieval of relevant court information. The software has undergone several upgrades since then, alongside national and sub-regional training activities; and although JEMS has several modules, most of the Court staff only use the system mainly for:

- basic entry data relating to parties
- types of case actions (e.g. events, filings, etc.)
- scheduling of matters and associated printing of Cause Lists/Dockets.

4.3 In February 2013, the ECSC rolled out a pilot Internet version called AMANDA JEMS developed by the Canadian-based firm CSDC (who acquired PCSS Inc.), at the Court of Appeal Registry, with the expectation of significantly increasing accessibility of the JEMS data to all stakeholders in the court system. However, after three (3) years of use it was realised that the functionality, and reporting facility of this Internet version, were not up to par with the Courts' requirements.

4.4 The ECSC, USAID, and national governments made significant investments during the implementation of JEMS, in 2000. The initial investment in the software was approximately US$500,000, in addition to further monies spent from various Member States and donors for purchasing additional licences and product modules. Payments were made directly to the software developer and vendor (at the time), PCSS Inc., for the acquisition of JEMS and several of the JEMS-related modules. However, it was noted that many of these modules were not made readily available to the Member State countries, by the vendor.

4.5 Altogether over the past sixteen (16) years, the ECSC Member States and Territories, have expended over US$2.5 million for the procurement and maintenance of JEMS and related applications. Annual support for the system was initially US$27,000 but with the addition of more modules and the increase of licensed users, the annual support fee has increased to roughly US$60,000.

[4] *Eastern Caribbean Supreme Court, Proposal for a New E-filing and Case Management Application for the Justice of the Eastern Caribbean (Extract), August 2018*

4.6 **Intellectual Property Rights and Data Ownership**. The initial signed Licence Agreement from the contracted software vendor PCSS Inc., stated that it owned the JEMS software, and any modifications made to the software. Ownership included: copyright, industrial designs, patent, trademarks/trade secrets, or any other intellectual property rights pertaining to the JEMS software and JEMS-related Materials. Materials include: the object, source code (when applicable), and any JEMS user documentation.

4.7 The ECSC and Member States Courts are obligated to protect the software and Materials from unauthorised disclosure by agents, consultants, servants, employees, customers, and successors. The entities must use the software and Materials as outlined in the Agreement and only by the judicial staff; however, written consent for non-employees to use the JEMS system and Materials, could be granted by the software vendor.

4.8 The Courts cannot also sell, assign, lend, lease, or dispose of JEMS and its related Materials; the only persons allowed to execute any of the aforementioned, are those notified by the Permanent Secretary, Ministry of Legal Affairs, Home Affairs and Labour. If the Agreement is terminated or cancelled, the Courts will have to return all copies of the programme and the Materials in whatever form, including modified copies, within thirty (30) days.

4.9 However, the ECSC and the all Member States countries, own the information that is inputted, and is being stored, in the JEMS system.

CHAPTER 5 IT OPERATIONS

Capacity Management

5.1 **Client-Server network.** The JEMS application currently used by the ECSC is a Windows-based Client-Server Application. The implementation involved establishing servers at each High Court office in the sub-region. These servers provide JEMS access to local clients via Local Area Network (LAN) connectivity and remote clients such as out-district magistrates, via VPN connectivity.[5]

5.2 **System Capacity and Performance**. DITES roles was to assist with installation of the software on the judicial computer units; the IT Dept. currently hosts the JEMS server hardware by ensuring there is always a reliable source of power; provide and maintain the computer hardware and network connectivity to the server. Whereas, the ECSC IT Department's role is to provide effective capacity management with minimum usage of IT resources, such as IT staff and tools for monitoring analyzing, improving performance and reducing consumption of the JEMS network resources.

5.3 **Remote access to JEMS server.** DITES creates remote login user accounts and credentials for the ECSC IT Department and respective judicial department's JEMS SAs to have authorised remote access into the JEMS server. Each time the ECSC requires remote access to the server, permission has to be granted by DITES, for an audit trail of access. DITES does not grant remote admittance to third parties; for example, ECSC's external contractors.

Change Management

5.4 **Request for changes**. The judicial departments are able to request changes to the standardised JEMS forms to meet specific requirements. However, the ECSC IT Department is only able to implement minor changes and with authorisation from the contracted software firm. The contracted vendor is solely responsible for making any major changes to the JEMS software.

5.5 **Change Management initiative**. At the time of the audit, the Montserrat branch of the ECSC, and other Member State countries were in the process of replacing JEMS with an E-Litigation Portal for Courts solution; this is a web-based application was developed by the Singapore-based software company, CrimsonLogic. The Supreme Court, Office of the Attorney General, and the Department of Public Prosecution, staffs, including local Lawyers, underwent mandatory training during the week of February 28th, 2020 and the E-Litigation Portal was launched on 3 March 2020.

5.6 [6]The *E-Litigation Portal* has the capacity to provide Court users and other stakeholders with access to assigned services at any time from any location and on various types of Internet-enabled devices such as smartphones, tablets, laptops, and desktops. It is comprised of the following components/Modules:

---

[5] *Eastern Caribbean Supreme Court, Proposal for a New E-filing and Case Management Application for the Justice of the Eastern Caribbean (Extract), August 2018*

[6] *Eastern Caribbean Supreme Court, Proposal for a New E-filing and Case Management Application for the Justice of the Eastern Caribbean (Extract), August 2018*

- **Web Portal.** Through the web portal, all users, regardless of whether they are internal users such as judges or external users such as lawyers, or other authorities etc., will have access to the diverse array of court services offered in the E-Litigation system electronically. The portal will provide the E-Litigation system with a consistent look and feel and allow users to access the system via multiple devices. The E-Litigation web-portal will provide the functionality to allow administrators to manage the static content of the portal. The portal will also include the user registration process, where users/administrators will be guided by the system to complete the process in an intuitive and easy to follow manner.
- **Judges Portal.** In the proposed E-Litigation system, the judges will have a customised backend portal. For example, in the judges' portal, there will be an E-Calendar that manages the calendars of the Judges. The E-Calendar is used for checking of their availability throughout the lifecycle of the cases.
- **E-Filing.** An integral part of case management, users of the E-Litigation system shall be able to file a document for different case types for example civil and commercial disputes at their own convenience. The interfaces will be simple and easy to use, with step by step screens to help users navigate through the entire application process. Users can select or drag and drop files to the system for document upload. The system will perform validation and necessary background checking, and user will be directed to online payment once the checks are successful.
- **E-Notification.** The E-Litigation system will provide administrators the ability to manage the email and message templates for notification. The notification will be triggered based on the event, for example user registration. Besides receiving notification through an email, users will be able to view their messages and tasks once they log in to their account.

5.7 The Magistrate's Court staff was not included in the training sessions; however, it was indicated by the ECSC IT staff, that they would be instructed in the near future.

Problem and Incident Management

5.8 **Helpdesk Support.** The ECSC IT Department in St Lucia is responsible for providing helpdesk services to troubleshoot issues reported by the SAs. Depending on the complexity of the problem, the ECSC helpdesk personnel guides the local SAs either by phone, or via email, on how to deal with the issue(s). When these directives do not work, ECSC would then try to resolve the problem remotely; they also maintain the software via remote access.

5.9 The SAs do have remote access to the JEMS server but only for rebooting it whenever there is buffering caused by slow connectivity of the server, or if there is of loss of network connection. However, if the remote refreshing of the server is unsuccessful, the SA will contact DITES to perform a physical reboot of JEMS server; if the issue persists, the matter will be forwarded to the ECSC support service to be resolved.

CHAPTER 6 INFORMATION SECURITY

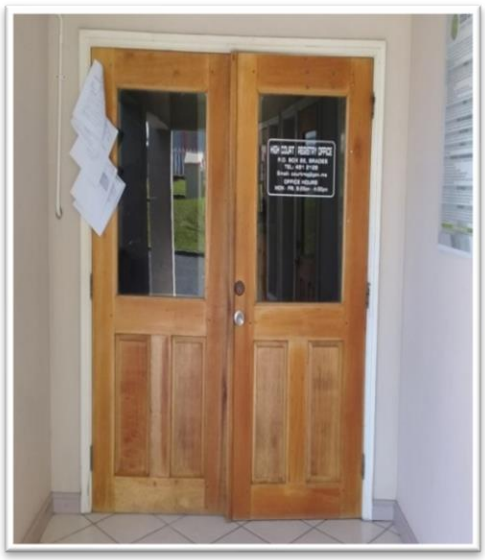
Confidentiality

6.1 **Non-disclosure of confidential information**. The software vendor and the Courts cannot disclose confidential information relating to the business or activities of either organisation; only to authorised individuals who were given permission by either Party and as per the terms under the Agreement.

6.2 **Third-Party entities**. When assistance is required from a third-party, and to whom confidential information has to be disclosed to perform their obligations, the software vendor must first receive the Licencee's approval and the third-party has to sign a binding non-disclosure agreement.[7]

Supreme Court Registry Office and Court Room

6.3 The solid concrete building that houses the Supreme Court/Registry and the High Court's courtroom was constructed in 2003; it originally accommodated other government sectors until the department occupied the two topmost floors, in January 2013.



Figures III & IV - Front doors of the Supreme Court Registry Office and Court Room

Physical Access Security Controls

6.4 **Points of Access**. There are two (2) points of access into the Supreme Court and Registry office. The main point of entry is via the front double doors; the clientele have unimpeded access during normal working hours and are not required to sign in or out. The open office space is small, therefore customers are always in the line of sight of either the Receptionist, or other members of staff, at all times. The second point of entry is designated for the private use of the presiding High Court Judge only; and is kept locked when not in use by the Judge.

[7] *Licence Agreement Between Professional Computer Software Services Incorporated (PCSS) And the Government of Montserrat*

6.5 The High Court's Room is located upstairs and has two (2) points of entry at the front and rear of the building, both doors can be used by the public once the High Court is in session. The flow of human traffic via the rear entrance is actively monitored by the Bailiff during court proceedings.

6.6 The GoM has a policy for all the keys of the various departmental buildings, to be held at the Brades Police Station. It is the responsibility of the GoM Brades Headquarters, Facilities Manager, to sign for these keys and unlock the buildings in the mornings, and to secure them after working hours. The Registrar possesses a personal set of keys for the Supreme Court.

Subsequent Events

6.7 The entrance of Supreme Court/Registry building was modified July 2020 to control access into the main office.

Environmental Security Controls

6.8 **Direct sunlight and dust.** The single hung windows in the building outfitted with dark green vertical blinds shields the office interior and computer equipment from the direct rays of sunlight; as well as providing some modicum of privacy. It was also noted that the lower halves of some of the windows were tinted with film for enhanced privacy. These windows are however not sealed against dust.

6.9 **Air-conditioning**. The computers and other office equipment located in the main office space and the private offices are kept cool by air conditioning; except for the only enclosed Administrative staff area. The a/c unit in this section does not work; however, it was disclosed that there are plans for its replacement.

6.10 **Protection against inclement weather**. The responsibility for securing all of the GoM buildings when there is a threat of a hurricane is a joint collaboration of the Office of the Deputy Governor (ODG) and the Public Works Department (PWD). A local contractor with the proper ladders and power tools is hired to bar all windows and doors for the GoM's multi-storied buildings.

6.11 **Flooding**. The building is not prone to flooding as it was built on sloping land which enables drainage of the rain water.

Magistrate's Court Building

6.12 The building that houses the Magisterial Department was constructed circa 1998/1999, along with other temporary offices, on the Government Headquarters compound. The building is made from prefab material with plywood flooring and interior wall paneling.

Figures V & VI - Magisterial Department Building

Physical Access Security Controls

6.13 **Points of Access and Control policies.** There are only three (3) frontal points of access in and out of the Magistrate's Court office; one of which is designated for public use; there is no rear entry. The office space is very compact and not subject to a large influx of clientele; it is therefore not necessary for persons to be signed in or out.

6.14 The GoM HQ Facilities Manager is responsible for unlocking and closing up the office and court house; however, the Magistrate and the most Senior Clerical Officer both have individual sets of keys for the building.

Subsequent events

6.15 During the COVID-19 lock-down period a customer service window was installed to control the number of people entering the Magistrate's Court office.

6.16 **Security System.** Similar to the Supreme Court, this building does not have a security system for the detection and deterrence of breaking and entering, and to alert nearby law enforcement. There is regular night patrolling of the GoM Headquarters compound by the Police.

Environmental Security

6.17 **Dust and direct sunlight.** The windows are glass louvers that are not sealed against dust; however, they are all equipped with vertical blinds for shielding the interior from the direct rays of the sun and for privacy.

6.18 **Air-conditioning.** The Magistrate's Court offices and office equipment are kept very cool by air conditioning units. At the time of the audit, it was observed that although the Executive Officer's a/c unit was working; reportedly it was in dire need of maintenance, therefore it was kept off.

6.19 **Protection against inclement weather.** The ODG and PWD are conjointly responsible for securing the window and doors of the Magisterial Department building whenever there is the threat of inclement weather. The covered overhang that runs the entire length at the front of building provides added protection.

6.20 **Flooding.** The building is not prone to flooding as the structure was elevated on sloping land. Secondly, the surrounding grounds of the GoM's Headquarters compound, has very good drainage.

CHAPTER 7 APPLICATIONS CONTROLS

Logical Access Controls

7.1 **JEMS user accounts.** Names of sanctioned employees are submitted to ECSC from all the judicial offices of the OECS member states, and user accounts are created and activated by the ECSC's IT department, in St Lucia. Each user account is assigned or linked to these individuals and a listing kept by the ECSC.

7.2 **Access Control to JEMS.** Access to JEMS is controlled via the JEMS application being installed only on the computers of approved users who are registered at the ECSC in St Lucia. Therefore, the system cannot be accessed from another workstation or device, within or beyond the offices by users or unauthorised personnel. However, if JEMS users do not properly safeguard their GoM login user ids and passwords, unsanctioned persons can gain access to the JEMS application once they bypass the DITES login window.

7.3 **Audit Trails**. Audit trails are generated, of all activities executed in JEMS, are recorded by the system. For example, when the JEMS application is accessed the date, time and name of authorised user; any changes made to the data; creation of case files; closing or archiving of the case files.

Input and Processing Controls

7.4 Authorised users perform JEMS-related tasks speedily and efficiently by selecting Graphical User Interface (GUI) pop-up windows or forms, with various icons and control elements for the insertion and capture of information and codes, and the organisation of data. For example:

- drop-down menus with options
- linked lists
- tabs representing other forms
- label buttons
- check boxes
- radio buttons
- white and yellow highlighted fields or text boxes

Specific text boxes are mandatory; that is, the system will not allow the user to move on to a resultant window, save, or close a Case file, until they are completed.

7.5 **Case File numbers**. New case files numbers are automatically generated sequentially, by the JEMS system. At the beginning of each new year the system restarts this unique sequential numbering format that includes: each country's identifying code, departmental code (Supreme or Magistrate's Court), the current year, and the number.

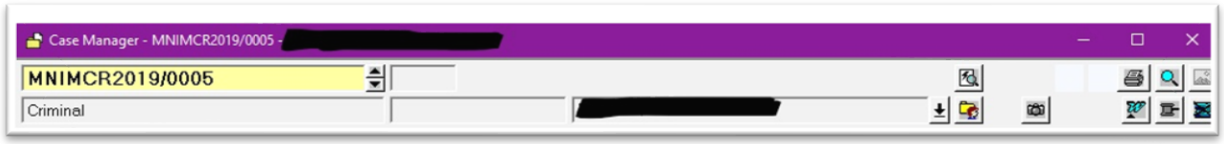


Figure VII - Sample of Montserrat Magistrate's Court Case File Numbering

These unique numbers are for reference purposes; they are hand-written on the hard copies of complaints filed at the Courts, in the Courts logbooks and registers, and on the court docket folders.

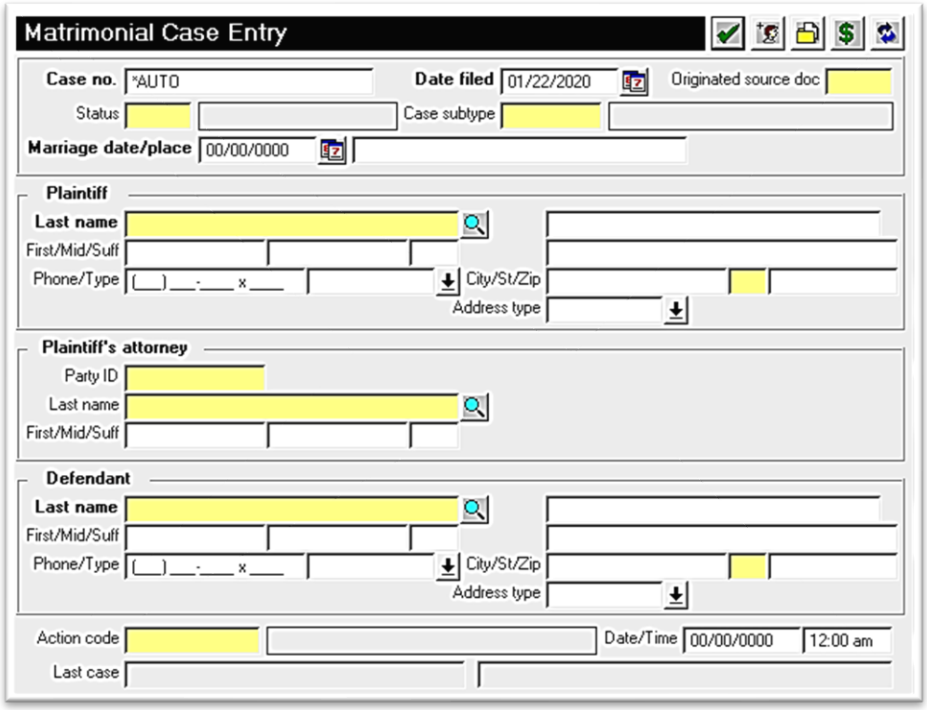
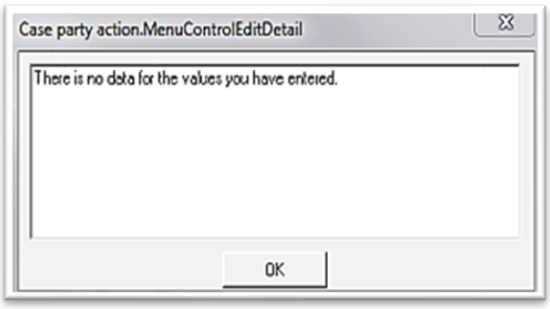
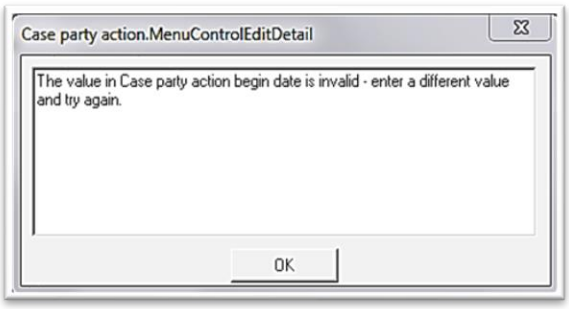
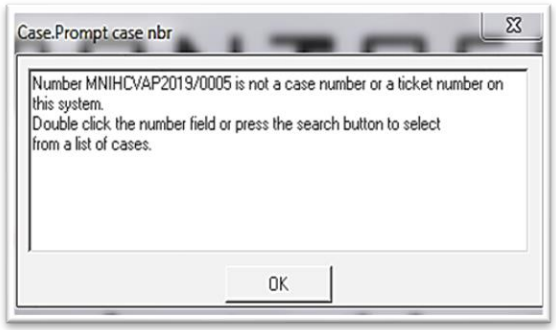


Figure VIII - Blank sample JEMS Case Files Form with various GUI input options

7.6 **System generated messages.** The JEMS system has input validation parameters that generate error messages and processing prompts, whenever invalid information is inserted in text field, transactions are incomplete, or information is required, and so forth.







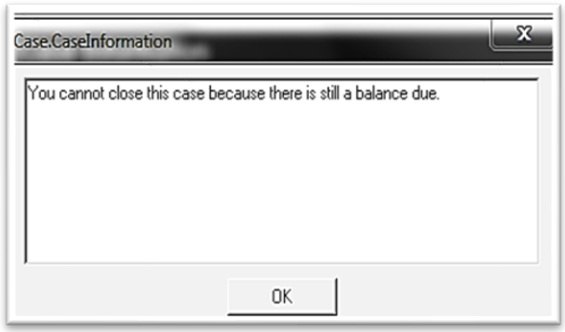


Figure IX to XII - Sample JEMS system generated messages

7.7 **Segregation of Duties.** Segregation of duties is used in both judicial departments to perform routine job responsibilities as per each employee's job function. This includes JEMS-related activities as follows:

JEMS Data Entry Clerks

1. Data Entry clerks can only perform the following tasks in JEMS:

- Create new cases
- Input the data into JEMS from the source documents and registers
- Update and close cases files; the Data Entry Clerks cannot delete case files.

JEMS System Administrators

2. The JEMS SAs perform the following tasks in JEMS:

- Input data
- Delete errors
- Amend information in text fields
- Upload and update the software library
- Responsible for reporting
- Troubleshoot minor input problems
- Remote reboot respective VPN server

7.8 Deletion of case files; this task is password protected and the SAs must provide a reason in the text box of the Dialogue Window that appears.

Output Controls

7.9 **Generating and Printing Reports.** Reports for all court matters are generated by the SAs only for ECSC in St. Lucia (with the exception of Court of Appeals). The data is extracted into Excel spreadsheet and emailed to them. In the case of Court of Appeals filed in Montserrat, the documents are sent via courier to ECSC, who inputs the information into JEMS extracts the data, and generates reports. They however, confer with Montserrat to ensure that the information in these reports is identical.

7.10 **Export of Scheduling Matters**. When Matters (Criminal, Civil, Probate, etc.), to be heard in court for a particular day or month, are entered into the JEMS a Cause List is generated and exported into a *.pdf* (Portable Document Format) document file. This *.pdf* file is emailed to presiding Judges or Masters, local lawyers, and other stakeholders; a copy is also emailed to the ECSC to be published on their website. The Cause List is sometimes printed and disseminated for internal use.

CHAPTER 8 BUSINESS CONTINUTY AND DISASTER RECOVERY

Business Continuity

7.11 **Back-up power supply.** All of the Supreme and Magistrate's Courts' computer and electrical equipment are plugged into heavy duty Uninterruptible Power Supply (UPS), except for one computer and a heavy duty Canon combination photocopier/printer/scanner at the Supreme Court. However, it was noted that the dedicated UPS for the Deputy Registrar's computer malfunctioned; the all-in-one printer does not have its own UPS and is plugged directly into a wall socket.

7.12 As with all the office blocks at the GoM Headquarters compound, the Supreme Court and Magistrate's Courts buildings are also linked to the communal generator that provides ancillary power during brief or extended power outages.

7.13 **Backup of JEMS.** The ECSC's IT department in St Lucia is responsible for performing regular full system, and daily backups, of JEMS. DITES perform daily rotational backups of JEMS and other application softwares, databases, which run on their SQL (Structured Query Language) server.

Disaster Recovery

7.14 **Hurricane Preparedness Plan.** Both the Supreme and Magistrate's Courts have a *Hurricane Preparedness Plan*[8,9] which are normally reviewed and updated annually. Both disaster preparedness plans have measures in place for securing the departmental data and electrical office equipment as follows:

(A) **Electrical equipment.** The Supreme Court's staff, with the assistance of the technical officers from DITES, will disconnect all of the electrical office equipment and ensure that the electrical mains are turned off. After the passage of the storm and the building is deemed safe, the office will be restored to normalcy; the technicians from DITES will return to reconnect the computers and to ensure that they are in working order. From all accounts, the computer towers and monitors are placed on top of the desks, except for the heavy duty all-in-one printer which cannot be moved due to the compactness and layout of the office space. From all accounts, the staff is responsible for securing the electrical equipment with waterproof coverings, which they fortify with heavy duty tape onto the desks.

The Magistrate's Court's plan communicated that all of their electrical equipment will be disconnected, elevated, and covered with water resistant material; and removed as far as possible from all windows and doors. The main switches will also be turned off. It was indicated that DITES technicians are responsible for dismantling and reconnecting the computers. In addition, different types of waterproof coverings are used, depending on the intensity of the storms; that is, either garbage bags or individual pieces of tarpaulin. Heavy-duty tape is used to fortify the coverings onto the desks.

[8] *Supreme Court Registry Hurricane Preparedness Plan, 2019*

[9] *Hurricane Preparedness Plan, Magistrate's Court*

(B) **Backup of Data.** The Supreme Court plan highlights that the department does not perform a full back up of its data, as it is the responsibility of DITES. However, staff are to back up important files on the departmental *H: Drive* such as:

- Incoming and Outgoing Registers
- Staff Leave Register, etc.

The Magistrate's Court stipulates in their plan that the department's electronic data would be backed-up on memory sticks, to ensure the preservation of the department's information. However, it was pointed out by the SA that the department switched to using a portable hard drive for backups in the event of an emergency; it is safeguarded in a locked fireproof filing cabinet.

CHAPTER 9 OBSERVATIONS, FINDINGS AND RECOMMENDATIONS

Observations

9.1 **Outmoded version of JEMS.** The Montserrat judicial departments were still utilising the very outmoded version JEMS 6.0., at the time of the audit; they did not follow suit and advance to the web-based version AMANDA JEMS, like other Member States and Territories.

9.2 **JEMS installation.** JEMS was installed on all five (5) computers at the Magisterial Department; and the computer in the courtroom. The application is also installed on majority of the office computers at the Supreme Court Registry, as well as their courtroom computer. There are only three (3) authorised users from the Magistrate's Court, and two (2) from the Supreme Court, who are registered at the ECSC.

9.3 **User account login procedures.** JEMS user accounts do not have user id and password restrictions; access to the application is associated with DITES's individual user account login credentials for their computer (symbiotic). Therefore, once logon to a GoM computer is successful sanctioned JEMS users and unauthorised individuals, can click on the JEMS icon to gain access.

9.4 **Manual locking of computers and automatic time-out feature.** To prevent unauthorised access to JEMS information on the office computers, by all accounts, most of the judicial staff practice manually locking their computers before moving away from their desks by simultaneously pressing **ALT** + **CTRL** + **DELETE**.

9.5 In addition, the computers have either Microsoft Windows 7 or 10 editions of the software, installed. These versions of the software have a default automatic time-out feature that locks the computers after a set period of inactivity. Subsequently, within ten (10) minutes of inactivity, the monitor will go blank; after an additional 30 minutes of idling, the computer will lock itself. In both instances the user is required to log back in with their user id and password.

9.6 **Security of Paper Court Records**. The documents filed at the court and closed ledgers with the duplicate information that was inputted into JEMS, are all stored in the judicial departments' relatively secured dedicated storage room areas.

9.7 **Client-Server Network Set-up**. There are client-server networks between (i) the Supreme and Magistrate's Court's courtroom computers and (ii) the Supreme Court Registry's, Court Reporter and Magistrate's Court, Court Clerk office computers. With this type of network architecture, the server has to be 'on' before a client computer can gain access to the information stored on the server. Therefore, the computers (servers) in either Court Room cannot be turned off in order for the Court Reporter and Court Clerk office client computers to have access to the *Liberty Court Recorder* application installed on the servers. These Court Room computers (or servers) are password protected.

9.8 **Update of Hurricane Preparedness plan**. Disaster preparedness plans are to be updated every year; the Supreme Court updated their plan in 2019, whereas the Magistrate's Court last updated, was in 2018.

Findings

Supreme Court Registry & Court Room

9.9 **Lack of early fire detection and suppression devices and equipment**. The Supreme Court Registry office is not outfitted with smoke detectors, fire alarms, or fire extinguishers. Upstairs in the Court room, there is one (1) mounted dry powder fire extinguisher, which has not been tested in recent times. There is also a second similar cylinder stored on a shelf in the Court Room's kitchenette; however, staff is unaware if it is working, considering that it was inherited from one of the former occupants.

9.10 The absence of early detection devices and warning system, and fire suppression equipment in either of the judicial offices, has the potential to have disastrous outcomes in terms of loss of human life, judicial, and historical information; in particular the Supreme Court Registry, which retains volumes of irreplaceable historical records of Montserrat's Births, Deaths, and Marriages, dating as far back as the 19th century. Lessons have not been learned from the double arson attacks on the Magistrate's and High Court courtrooms on 3rd December, 2012; these fires could have been detected early and suppressed before damage was done to the buildings, court computers, and stenographer machine, being housed in the courtrooms.

9.11 **Lack of Physical Access Security Controls for Court Room.** The front door at the lower level entrance of the Court Room is left unlocked and unmonitored when there is no court. This practice is done mainly to accommodate Supreme Court Registry staffs who sometimes retrieve files or documents from the High Court Reporter or from the storage cupboards located on the landing outside of the Court Room.

9.12 This unlocked door observance extends upstairs in the actual Court Room where doors leading: (i) from the courtroom into the Court Reporter's office, and (ii) in and out of the communal restroom area, remain open once there is no High Court. The Court Reporter however, does take the added precaution of locking the outer door between the courtroom and restroom area, when using the facilities.

9.13 The practice of leaving these doors unlocked is very risky, as it leaves room for prospective unauthorised individuals to:

- gain unlawful access to High Court documentation
- damage or destroy the court room and property within
- conceal weapons or dangerous devices inside the court room
- perpetrate bodily harm to the Court Reporter.

Figure XIII - High Court's Court Room landing

9.14 **Compromised windows.** During the inspection of the upper levels of the building designated to the Supreme Court Registry, it was noted that the entire building is outfitted with single hung windows that are not hurricane impact resistant. Some of them are in various stages of disrepair as shown below in *Figures XIV to XVII.* It was also apparent that when the building was originally constructed some seventeen (17) years ago, all of the windows were equipped with outer wooden hurricane shutters. These wooden shutters, with the exception of one window, were removed to accommodate the hurricane preparedness measures performed before impending inclement weather.

Figures XIV to XVII - Windows in various stages of disrepair

9.15 **Water damage**. The rear section of the Supreme Court's office has widespread damage due to water leakage spanning from the Conference Room/Library, to the Judge's Chambers. Notably, there is brown discolouration on the white ceiling panels; water on the tiled floors and oozing beneath the wall; considerable peeling of paint; warped sideboards (some of which have been removed). There is similar damage upstairs in the Court Room.

Figures XVIII & XXI - Evidence of water seepage in the Supreme Court Building

Magisterial Department

9.16 **No early fire detection and suppression devices and equipment.** The entire Magistrate's Court block is not outfitted with smoke detectors, fire alarms, or fire extinguishers.

9.17 **Insufficient computer resources.** The Magistrate's Court Executive Officer/JEMS SA computer malfunctioned months prior to the audit, and it was temporarily replaced initially with the computer unit from the Court Room, then later on with a temporary loan of a laptop from DITES. However, the laptop's specifications did not meet the system requirements for the operation of the JEMS software; therefore, the SA was unable to gain access to JEMS.

9.18 **Data input issues.** The Data Entry Clerk, who had access to JEMS, was unable to record specific court case information as the task required prior modification to be done by the SA. For example, whenever new laws and regulations are passed, or fines/charges are

changed, the SA has to update JEMS with this latest info. As a result, JEMS-related activities at the Magisterial Department were virtually at a standstill.

9.19 **JEMS access issues.** At the time of the audit, only one of the two (2) Data Entry Clerks could gain access to the JEMS server to input court information into the system; the second user was being notified by the system that the department was over its limit of contractual users.

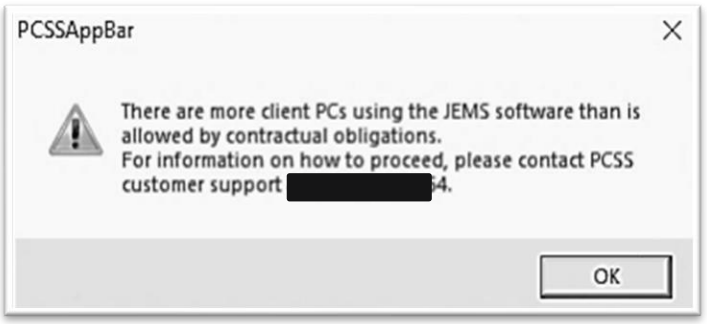


Figure XXII - JEMS System Notification

Subsequent events. This access issue has since been rectified by the ECSC IT department.

9.20 **Non-Termination or Change of Employment policy.** When registered JEMS users depart from either judicial department, the System Administrators do not notify the ECSC IT Dept. There have been six (6) collective leave-takings over a period of over seven years, and their user accounts are still active.

9.21 **Shortcomings and Issues of JEMS outlined by ECSC**. Although the JEMS application and client-server architecture benefited the operations of the various branches of the ECSC across the region, the St Lucia-based organisation highlighted the following drawbacks:

(i) The ECSC IT staff had to travel to each Member State country to provide server-related support.

(ii) In order to make JEMS available at the remote court offices, several other hardware and software solutions were required.

(iii) Each Member State's database has to be managed and backed-up individually.

(iv) There were several unresolved 'bugs' in the application that were not corrected and therefore negatively impacted Court processes.

(v) Over the years, several of the upgrades had glitches such as loss functionality of some of the components of the software; and temporary unavailability of the data. Furthermore, upgrades proved to be challenging, as they had to be applied separately on each Member State's server and clients.

(vi) It was a huge challenge for the ECSC IT Department to maintain complete, safe, and secure control of Court data, due to the dispersion of the various servers and databases across each Member State.

(vii) The JEMS servers are currently being managed through remote administration applications, and software related issues are usually resolved within 24 hours. However, some of the hardware issues have to be outsourced when the travelling ECSC

IT personnel cannot resolve them. Furthermore, the IT Department is unable to assure users of a 99% up time of the servers.

(viii) The Canadian-based software vendor CSDC Inc. (that acquired PCSS Inc.) that created the web-based solution AMANDA JEMS was not willing to make any improvements to the software. [10]

Recommendations

9.22 **Procurement and installation of fire suppression apparatus.** We are strongly recommending that the Supreme and Magistrate's Courts invest in at least 1 or 2 canisters of either foam and/or powder fire extinguishers to reduce the risk of human life and loss of irreplaceable historical records and information.

Subsequent Events. The Magistrate's Court procured a smoke detector for the courtroom, and have consulted with the Fire and Rescue Services about the acquisition and installation of fire extinguishers for both the main office and courtroom.

9.23 **Implement Physical Access Security protocols**. We strongly recommend that management at the Supreme Court Registry should consider implementing the following protocols for controlling access to the Court Room:

(i) Keeping the lower level main front door locked once the High Court is not in session in order to restrict unauthorised personnel from entering the Court Room. Only the Supreme Court staff should have access with a key, whenever the department requires documentation from storage, or from the Court Reporter.

(ii) The second option is to install a swipe key card system, which will produce an audit trail of who and when entered/exited the building.

(iii) To visit with the Court Reporter, one must report to the Supreme Court's reception area. The person(s) can either be escorted to the landing; or gain access by Reception and be directed upstairs at the meeting area (landing), then escorted through the Court Room into the Reporter's office.

9.24 **Effect Termination and Change of Employment policy.** As a further precautionary IS measure, we are advising both JEMS System Administrators to commence formally notifying the ECSC IT Dept. via email, when registered authorised users of JEMS leave either judicial department. Requests should be made that their corresponding user accounts be deactivated.

Subsequent Events. The six active accounts of persons that were no longer within the Department were made inactive.

9.25 **Replacement of Magistrate's Court JEMS SA Personal Computer.** We recommend that the Magistrate's Court continue to liaise with DITES and lobby for a replacement computer as soon as possible, to enable the JEMS SA to resume oversight of the JEMS application.

Subsequent Events. The investigative aspect of the audit was completed two weeks before the island went on locked down due to the COVID-19 pandemic; as a result, the finalisation

[10] *Eastern Caribbean Supreme Court, Proposal for a New E-filing and Case Management Application for the Justice of the Eastern Caribbean (Extract), August 2018*

of the audit report was delayed. However, since the re-opening of the Government offices in May 2020, the Magistrate's Court JEMS System Administrator received a new computer; JEMS version 6.0 was installed on all of the department's computers, to include the computer in the courtroom.

9.26 **Backup power supply and Power surge protection.** A replacement heavy-duty UPS is required for the Deputy Registrar's computer. In addition, a surge protector is required for the conservation of Supreme Court's large, costly, all-in-one photocopying machine, from damaging power surges and low voltage occurrences.

9.27 **Update of Disaster Preparedness and Business Continuity Plans.** To ensure the seamless continuity of the Supreme Court Registry's IT operations after a storm or hurricane, we advise the Supreme Court to emulate the Magisterial Department and invest in a portable hard drive with a minimum 2 Terabyte (TB) storage capacity for backing up their important departmental electronic data.

9.28 We are also encouraging the Magistrate's Court to update their Hurricane Preparedness Plan on an annual basis; and any changes that took place since 2018 should be included in the plan. For example, the switch from using memory sticks to a portable hard drive.

CHAPTER 10 MANAGEMENT RESPONSES

10.1 Both the Supreme and Magistrate's Court did not submit any Management Responses to the observations, findings, and recommendations.

CHAPTER 11 AUDIT CONCLUSION

11.1 The Office of the Auditor General (OAG) has determined from this General IT audit that although outmoded, the JEMS 6.0 Case Management software has benefitted the Montserrat Supreme and Magistrate's Courts by facilitating the generation of court dockets, detailed scheduling with conflict-checking, reporting, and prompt sharing of information. The application is adequately secure, and it provides for the accurate input, secure storage, organisation, and retrieval, of Montserrat's court information.

11.2 The majority of the objectives of this General IT audit, pertaining to IT Governance and Operations; Development, Acquisition, and Outsourcing; Business Continuity and Disaster Recovery; Application Controls; and Information Security, were met. However, weaknesses were identified under the areas of Information Security, IT Operations, and Business Continuity and Disaster Recovery.

11.3 We the OAG conclude that it would be in the best interest of the Montserrat Supreme Court Registry and Magistrate's Court, to consider and address the inadequacies and the recommendations that were highlighted.

REFERENCES

Web Pages

https://www.calytera.com/courts-justice/judicial-enforcement-management-system/

https://discovermni.com/2018/09/21/eastern-caribbean-courts-going-digital-with-elitigation-system/

https://www.eccourts.org/eastern-caribbean-supreme-court-fifty-1967-2017-justice-don-mitchell-ret/

https://www.eccourts.org/implementation-of-an-e-litigation-portal-for-courts-in-the-eastern-caribbean/

https://slideplayer.com/slide/5770134/

https://youtu.be/OQYCzuAmpCY

Books

INTOSAI WGITA IDI Handbook, IT Audit for Supreme Audit Institutions, February 2014

APPENDICES

APPENDIX I - Examples of the Montserrat Courts JEMS Application Bars