

5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128



31415926535 8979323846 2643383279
5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128

RAUSCH
ADVISORY SERVICES

43383279
0974944
8034825
2306647
9408128



31415926535 8979323846 2643383279
5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128

September 7, 2018

Ms. Connie Brown
Executive Director, Office of Internal Compliance
Atlanta Public Schools
130 Trinity Avenue, S.W.
Atlanta, GA 30303

Ms. Brown,

Rausch Advisory Services ("Rausch") is pleased to present the results of the 2018 Information Technology General Controls review.

The review was performed March 30, 2018 through April 20, 2018 timeframe. The Executive Summary includes the scope, objectives, methodology, approach, and observations of the engagement as well as overall recommendations for Atlanta Public Schools ("APS").

Rausch appreciates the opportunity to have assisted in the review. If you have any questions or comments, please contact us at 404-775-1151.

Respectfully,

Michael Lisenby
Managing Partner
Rausch Advisory Services, LLC.

Table of Contents

Background	4
Objective, Scope and Methodology.....	4
Executive Summary	5
Issues and Recommendations.....	6
Observations Table.....	6
Observations, Recommendations and Management Response	7
1. Business Impact Analysis & Disaster Recovery.....	7
2. Logical Access.....	8
3. 2015 Information Technology Risk Analysis Review	10
4. Vulnerability Analysis and Penetrating Test.....	10
5. Information Security Management System (ISMS) Framework	11
6. Outdated Documentation.....	13
7. Backup and Restore Controls.....	15
8. System Development Life Cycle Controls.....	16
9. Data Center Environmental and Security Controls.....	17

Background

Rausch Advisory Services (Rausch) was engaged by the Internal Compliance Department of Atlanta Public Schools (APS) to complete an information technology general controls (ITGC) review. Rausch performed the review between March 30, 2018 through April 20, 2018. The executive summary included below summarizes the objectives, scope and observations of the engagement, as well as overall recommendations for APS.

We conducted this audit in accordance with Control Objectives for Information and Related Technologies (COBIT) auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We limited our work to those areas specified in the “Audit Objective, Scope, and Methodology” section of this report.

Objective, Scope and Methodology

The objectives of an information technology general control review were to provide APS with a high level of assurance that the information technology controls are adequately designed by ensuring security, confidentiality, availability and integrity of corporate data. Specifically, we sought to assess APS’s data security environment, data back-up and disaster recovery processes, logical access review, program change management and system development life cycle.

To meet our objectives, we reviewed various documents and processes including:

- ✓ Access Control Regulation v03152014.docx
- ✓ APS Application System Contingency Plan- Lawson and AIX.2-20-15.docx
- ✓ APS Board Policy - Internet Acceptable Use Policy - IFBG.PDF
- ✓ APS Board Policy - Use of Electronic Devices by Students Policy - JCDAF.PDF
- ✓ APS Malware Protection Standard.docx
- ✓ Atlanta Public Schools IT Disaster Recovery Incident Response Plan - March 2014.docx
- ✓ Catalog New Work Intake Process Draft v3.vsd
- ✓ Corporate Asset Classification and Control Policy_riversedits526.docx
- ✓ Corporate Communication and Operations Management Policy_priversedits526.docx
- ✓ Corporate Compliance Policy_riversedits526
- ✓ Corporate Information Security Policy_riversedits526.docx
- ✓ Incident and Response Policy_edited524.docx
- ✓ IPS Monitoring Strategies2.docx
- ✓ Portable Technology Use Agreement. IMapdocx.pdf
- ✓ SDLC methodology.doc.docx
- ✓ Software Development Life Cycle (2).doc.docx
- ✓ Visio-Catalog New Work Intake Process Draft v3.pdf

The Rausch professional interviewed APS personnel, which was particularly useful since several of the written policies were either in draft or out of date and certain processes were not yet documented. The following is a list of interviews we conducted during our review:

- ✓ Aleigha Henderson-Rosser, Executive Director Instructional Technology
- ✓ Alisa Morningstar, Executive Director Purchasing
- ✓ Cathy Rollins, IT Policy and Governance
- ✓ David Lis, Assistant Director ERP Apps
- ✓ Ifiok Moses, Identity Management Engineer
- ✓ Karen Wright, IT Service Operations Manager
- ✓ Laurence Warco, Legal Counsel
- ✓ Michael La Mont, Executive Director, Data & Information
- ✓ Nate Dogan, Infrastructure Specialist
- ✓ Olufemi Aina (Femi) Executive Director IT
- ✓ Roanna Washington, Director of IT Security and Network Services
- ✓ Sam Pointer, Director of Infrastructure
- ✓ Skye Duckett, Chief Human Resources Officer
- ✓ Tameka Barber, Applications Director
- ✓ Veronica Wells-Haven, Oracle DBA

Through the course of the review, Rausch identified gaps within APS ITGC's and has provided a roadmap for remediation and the development of an effective IT program; containing both the definitions and the practical guidance necessary for assessing and mitigating risks within the IT environment. This is included as our Issues and Recommendation section below.

Executive Summary

Rausch observed that APS overall ITGC governing controls are based on industry best practices. However, there are ad hoc procedures currently utilized to operate APS's infrastructure. Based on our interviews, observations, reviews of documentation and review of previous assessments performed, Rausch's evaluation of the design and operating effectiveness of the ITGC's identified nine opportunities for improvement.

The most significant observation is APS's Disaster Recovery (DR) plans are incomplete and evidence of recent testing of the DR plans was not provided. Additionally, there is no evidence that a Business Impact Assessment was performed to set Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) by the business units within the DR plans.





Without complete and regular testing of the DR plan against all critical applications, IT may not be able to restore the system to its former pre-disaster state; IT may not be able to understand and connect to its third party providers; IT may not be able to connect to its disaster recovery testing center; IT may not have an understanding of the priority for restoration of applications/connections to internal applications; IT staff may not have a clear understanding of their roles/responsibilities in the event of a disaster; interfaces may not be understood and connections may not be completed correctly or in a timely manner.

We concluded with a reasonable level of assurance that the current disaster preparedness plans for critical applications would NOT satisfy the business defined RTO and RPO goals that would need to be established by the necessary departments.

This report is intended solely for the use of management and should not be used for any other purpose.

Issues and Recommendations

Risk Level Key

-  **High Risk:** matters and/or issues are considered to be fundamental to the mitigation of material risk, maintenance of internal control or good corporate governance. Action should be taken either immediately or within three months.
-  **Medium Risk:** matters and/or issues are considered to be of major importance to maintenance of internal control, good corporate governance or best practice for processes. Action should normally be taken within six months.
-  **Low Risk:** A weakness which does not seriously detract from the internal control framework. If required, action should be taken within 6 -12 months.
-  **Informational:** The identified Informational level findings are not considered risk but may contain valid and useful information that may aid APS with process improvement.

The table below summarizes the observations, the potential risk level and when management anticipates corrective action to be implemented. Detail on the steps required to address the observation is provided in the “Recommendation” section for each item with reference to the corresponding NIST standard. (APS IT has adopted National Institute of Standards and Technology ‘NIST’ standards and practices.)

Observations Table

Number	Observation	Risk Level	Est. Completion Date
1.	Business Impact Analysis & Disaster Recovery	High	Mar 2019
2.	Logical Access	High	Dec 2018
3.	2015 Information Technology Risk Analysis Review	High	Jun 2019
4.	Vulnerability Analysis and Penetration Test	High	Jun 2019
5.	Information Security Management System (ISMS) Framework	Med	Jun 2019
6.	Outdated Documentation	Med	Jun 2019
7.	Backup and Restore Controls	Med	Jun 2019
8.	System Development Life Cycle Controls	Med	Jun 2019
9.	Data Center Environmental and Security Controls	Med	Jun 2019

The observations of our review along with our recommendations for process improvement with management's response and implementation timeline are presented on the following pages.

Observations, Recommendations and Management Response

1. Business Impact Analysis & Disaster Recovery

Rausch noted two polices "Atlanta Public Schools IT Disaster Recovery Incident Response Plan" - dated March 2014 and "APS Application System Contingency Plan - Lawson and AIX" – dated February 2015 are outdated. Also, Rausch was informed by the Executive Director of IT there are no recovery procedures or hardware in place at the hot site to recover the Lawson financials. Rausch reviewed the current plans in place and determined that it does not contain RPO's or RTO's established by the business units.

Risk

The objective of a disaster recovery plan is to minimize downtime and data loss. The primary objective is to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable. The plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will result in normal operations for the organization.

Recommendation (NIST: CP-4 Contingency Plan Testing)

Rausch recommends APS conduct a Business Impact Analysis (BIA) with each business unit to determine and evaluate the potential effects of an interruption to critical business operations because of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis, which describes the potential risks specific to the organization. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of resources in the wake of a disaster.

The BIA report will identify the RTO and RPO's. The RTO is the time within which a business process must be restored, after a major incident has occurred, to avoid unacceptable consequences associated with a break in business continuity. The RPO is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down because of a major incident.

Once a BIA is completed, and the RPO's and RTO's are established, the DR Plans will need to be updated to reflect all systems and scenarios identified. Additionally, Rausch recommends a policy be developed stipulating periodic testing should be performed at least annually. Such a plan would be based on various disaster scenarios and likelihoods of occurrence.

Management's Response

In light of the changes in the architecture over the past four years, *the team has begun a process of updating* the Disaster Recovery & Business Continuity Plan this school year to reflect the recent changes. The document will also include a reassessment of the Business Impact Analysis (BIA) as well as RPOs and

RTOs. It will be modified to include the individualized system prioritization for the critical applications/systems.

The current RTO's for onsite critical systems/applications range from 0 (immediately) to 24 hours:

- ◆ Network Infrastructure - Location(s) CLL and Telex - Priority 1 RTO 0
- ◆ Databases (SQL & Oracle) - Location (CLL) - Priority 1 RTO 2hrs.
- ◆ Lawson (Financials) - Location (CLL) - Priority 2 RTO 8hrs.
- ◆ Email - Location (CLL) - Priority 2 RTO 8hrs.
- ◆ Phone System - Location (CLL) - Priority 3 RTO 8hrs.
- ◆ Lenel Door Access - Location (CLL) - Priority 3 RTO 8-12hrs.
- ◆ MSC (Nutrition) - Location (CLL) - Priority 7 RTO 24hrs.
- ◆ Edutracker/Edulog (Transportation) - Location (CLL) - Priority 8 RTO 24hrs.
- ◆ SharePoint - Location (CLL) - Priority 9 RTO 24hrs.

Anticipated Completion Date - March 2019

2. Logical Access

Rausch discussed and observed the user provisioning process for active directory access from interviews with the APS Identity Management Engineer. The Student Information System (SIS) and Infor Global Human Resources (GHR) each have an interface into Active Directory (AD). The interfaces for the student and staff user provisioning and de-provisioning have separate automated processes to assign AD Accounts, Organization Units (OU) and AD groups into two separate APS domains. Contractor access to AD and approved system access above AD for Lawson financials and human resources, as well as privileged administrator and VPN access require an approval from a supervisor. Staff other than teachers, assistant principals and principals require approval to SIS. Each of these access requests has their own separate SharePoint form that is filled in and routed through workflow for approval. Rausch notes there is no escalation and notifications designed into each of these current SharePoint workflow processes. Rausch was also informed during several interviews there is no process in place to review access privileges for staff that transfer positions. Rausch noted these processes were not documented.

Risk

- A. Inadequate granting, monitoring and removal of network access exposes the organization to the following risks:
 - a. Segregation of duties - a user having unnecessary or excessive access to applications or privileges could result in compromise of the integrity of the process or allow an individual to potential to commit fraud.
 - b. Access to sensitive or critical functions and data – A user having access to sensitive data such as employee personal information, organization confidential data or intellectual property of the organization may be able to compromise the integrity of the process or inappropriate use

and gain further access to sensitive data.

- B. Privileged accounts have admin privilege to network, data, and software of the organization and should be restricted considering the principles of least privileges based on business needs and segregation of duties considerations. Privileged user account holders may be able to manipulate, delete or hide information processing facilities under their direct control. Elevated access exposes the organization to erroneous activities, system sabotage or fraud.

Recommendation (NIST: AC-2 Account Management)

Rausch recommends APS document the Active Directory (AD) user/deprovisioning process and architecture. Include naming conventions, interfaces and files. Complete an inventory of AD Organization Units (OU) and ensure they align with APS location naming convention. Complete an inventory the AD groups and special privileges assigned to these groups. Identify which OU and groups are part of the AD user/deprovisioning process. Rausch recommends the following steps:

- 1) APS should document the special access processes for granting and removing user access to systems and applications that are not covered under the automated AD user, provisioning/deprovisioning process.
- 2) Workflow, escalation and logging should be developed for addressing user access request.
- 3) APS should develop and document a periodic user access review process for AD users, system administrators, contractors, Infor Lawson applications, VPN and privileged access.

Management's Response

Since our last IT Security audit in 2015, the APS technology team has made some improvements to prevent unauthorized access to systems. These include but are not limited to:

- ◆ LAPS to control local Admin access on desktops.
- ◆ Multi-factor authentication (MFA) for VPN and the student Edgenuity application.
- ◆ Role-based access for GHR. Created new security groups and completed an entitlement audit to ensure that people don't have more access than they need to perform their duties.
- ◆ Group Policy in Active Directory to separate admin and standard user access to workstations and servers.
- ◆ Stealth Intercept and Stealth Audit to monitor elevated privileges and changes to Active Directory. Changes to AD are flagged and notification sent to the security team
- ◆ Exabeam "User Behavior Analysis" tool, to identify and flag suspicious login behavior

In addition, *there is an ongoing effort to actively review and cleanup accounts within active directory.* We will ensure that the procedures and documents flagged in this finding are spelled out in updated documentation to make it easier for a follow-up audit review.

Anticipated Completion Date - December 2018

3. 2015 Information Technology Risk Analysis Review

The APS IT department engaged the firm Lockstep Technology Group to perform an information technology risk analysis in 2015, with a final report delivered January 2016. The scope of the assessment identified and rated key IT assets based on confidentiality, integrity and availability. Their review followed the National Institute of Standards and Technology (NIST) cyber security framework. The goal of performing a NIST-based organization assessment is to understand the organization's security posture, as it relates to key business requirements, cybersecurity policies and existing risk management program. While performing a vulnerability analysis and a penetrating testing analysis, the report identified 74 risk and recommendations ranging from 45 high, to 22 medium and down to 7 low-risk items. Rausch received a project listing from the Project Management Office showing that 25 of the 45 identified high-risk items were completed and marked 100%, while the remaining high-risk items were at some stage between 0% to 50% complete.

Risk

These identified risks have the potential for loss, damage or destruction of an asset because of a threat exploiting a vulnerability. Testing for vulnerabilities is critical to ensuring the continued security of your systems by identifying weak points and developing a strategy to address the risk each pose to the organization. Equally, remediating the high-risk items in a timely order is critical to reducing APS' exposure.

Recommendation (NIST: RA-1 Risk Assessment Policy and Procedures)

Rausch recommends an inventory of identified risk and recommendations along with an independent risk review by the Office Internal Compliance to ensure proper closure of these items. The inventory should include managements response and controls to minimizes the risk posed by security vulnerabilities to students, customers, critical infrastructures, and the Internet. The independent review should validate the responses and applicable controls implemented to reduce exposure to the vulnerabilities. A timeline needs to be established to address all open items.

Management's Response

The APS technology team *accepts the recommendation* of the audit finding and will partner with the OIC to conduct independent reviews of the remediation status. It has been our plan to conduct assessments every two year. As planned, the team will engage a security vendor to conduct a re-assessment of the APS IT environment this school year to measure the effectiveness of the remediation efforts to date. APS IT has engaged Lockstep to perform penetration testing scheduled to start in October 2018.

Anticipated Completion Date - June 2019

4. Vulnerability Analysis and Penetrating Test

Rausch noted there has been several changes made to the APS network due to the information technology risk analysis performed the end of 2016 and the phishing attack that occurred during 2017. The last vulnerability analysis and penetration test were performed 2.5 years ago. There is not a formal schedule in place at APS to test the external and internal perimeter for potential vulnerabilities.

Risk

With no formal plan in place for performing penetration testing APS may not be able to identify, respond and react appropriately to different types of cybersecurity incidents. This could lead to continued potential breaches not being reported properly, excessive fines, reputational risk and network system downtime.

Recommendation (NIST: CA-8 Penetration Testing)

- 1) Rausch recommends APS document and perform an external risk assessment of their network on at least an annual basis.
- 2) As part of the risk assessment process – a penetration test will identify vulnerabilities in any web applications, internal devices, Internet-facing IP addresses and applications and link them to identifiable threats.
- 3) As part of the risk treatment – a penetration test ensures that controls work as designed.
- 4) As part of the continual improvement process – a penetration test ensures that controls continue to work, and that new threats and vulnerabilities are discovered and fixed.

Management's Response

The APS technology *team accepts the recommendation* of the audit finding to perform Penetration Testing on a regular basis. Budget constraints, however, may affect our ability to conduct this annually as recommended. We will work with the OIC to negotiate agreed upon schedule (perhaps every 2 years). Also, APS IT has engaged Lockstep to perform penetration testing scheduled to start in October 2018.

Anticipated Completion Date - June 2019

5. Information Security Management System (ISMS) Framework ●

Rausch observed that APS has not implemented a standardized framework for an Information Security Management System (ISMS) – referred to as a security management program. An ISMS would provide a strategic program, policies and procedures for the systematic determination of security requirements, risks and designation of roles and responsibilities. Currently, this is an ad-hoc process at APS based on industry best practice. The risk of not having a formalized structure in place presents difficulty in managing the requirements, operation and improvement of the security management program.

Risk

Without formal processes and procedures in place, application of risk management and security controls may be applied inconsistently, leading to the risk of unauthorized access or increased risk. The issues noted in the remaining findings also further support the importance of establishing an ISMS Framework.

The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

Recommendation (NIST: 800-53 Risk Management Framework)

Rausch recommends the following steps to be undertaken by management to ensure such an ISMS program is implemented:

i. Framework for Information Security Management

Rausch recommends the adoption of an ISMS framework, one that is authorized by executive management, and based on international best practices – such as NIST – 800-53 or ISO/IEC 27001:2013, that clearly shows how management provides directives on managing information security risks, as well as provide an authorization statement that empowers a Management Representative (MR) to oversee and project manage the day-to-day running and implementation of the management system.

ii. Information Security Policy and Authorization Statements

To consolidate step (i) above, the appointed MR should help management put together a high-level document that expressly declares management commitment to information security by stating the organization's objectives and the requirement of interested parties. Additionally, the document should include the framework or standard to follow as well as declare the authority of the MR.

iii. Management Oversight

The MR should then champion the process of putting together an oversight committee for information security to include representation of stakeholders from across the enterprise. The oversight committee needs to be represented by a charter. The charter should focus on the management of Information Security risks, controls and improvement. The identified roles and duties of all participants (by function); from direct participants (both operational and non-operational) to supporting participants and third parties should all be formally documented in an Information Security Governance Plan.

iv. Information Security Program

Applying such a framework will facilitate the creation of a security program that affords value transparency and consistency in execution by formally structuring areas of responsibilities and present a pattern for highlighting dependencies across process areas, while relating them to roles involved in the life-cycle of information security at APS; from initiation to implementation to operation and improvement of security controls.

For effective risk management, a structured coordination of stakeholders, including risk, control and process owners should be implemented to ensure that historical and operational data are exhausted in determining APS's threat/vulnerability landscape. Thereby making control selection more representative of the organization's risk posture.

v. Risk Management

Still within the planning phase, management should approve a methodology for management of information security. This approved process provides a means of continuously assessing the

organization's risk posture against its risk appetite. This essentially will include predefined criteria for risk acceptance and mitigation strategies, applicable to both internal parties and processes, as well as those that may impact APS through suppliers and other interested parties.

Part of such a risk management program should be a documented and circulated Risk Treatment Plan to guide the selection, implementation and maturity of security controls.

vi. Knowledge/Document Management

The MR should oversee the implementation of a Documentation Hierarchy Pyramid (DHP) that will constitute a system for managing document requirements, development, applicability, communication and dissemination.

vii. Continuous Improvement

A clearly documented process should also be put in place for the activities of management in monitoring, reviewing and improving the security management program. For this, the MR must ensure the following:

- a. Work with Internal Compliance to identify the audit requirements of the ISMS as well as ensure periodic audits are conducted and reported to management.
- b. Coordinate with control and process owners to create baselines (metrics) for measuring the effectiveness of the process structures and controls involved in the management of security risks. This should also include detailed and dashboard-style reports to management.
- c. Develop a system for processing and responding to feedback from interested parties, as well create templates for reporting this to executive management such that issues can be tracked and tied back to controls within the management system.
- d. Corrective actions and opportunities for improvement are presented for management review and approval.

Management's Response

The APS technology team *accepts the recommendation* of the audit finding as best practice. While the current structure is not as formally documented as noted in the finding, many of the identified functions are being performed by a team of two employees to meet the needs of the school system. The recommendations would require a larger team and budget.

Anticipated Completion Date - June 2019

6. Outdated Documentation 

Rausch reviewed the documentation as noted in the executive summary and noted most are not up-to-date and there is no sign-off indicated. Rausch was informed by the Executive Director of IT there were technical writers brought in to create policies and procedures. However, Rausch did not receive any of these documents at the time of the review. Rausch was also informed by the identity management engineer that there is now another technical writer on-site gathering processes and procedures from the

infrastructure team to create new documentation. Lack of documentation was a risk identified during the 2015 information technology risk analysis.

Risk

As there was no observed formal system of document creation, review, approval and dissemination. This results in an inefficient/non-repeatable process, missed opportunities for process improvement, non-compliance as well as loose accountability: For example:

- A. Not having documented procedures does not allow process owners and supporting participants a ready guidance from historical resolution.
- B. Lack of a top-down document management/control results in the creation of documents that get outdated before being approved or circulated. There’s also a lack of visibility into processes and methodologies. A framework such a Documentation Hierarchy Pyramid is required to provide control and guidance.
- C. Accountability for required processes is unattainable due to lack of procedure documents that match activities to their roles and responsibilities.

Recommendation (NIST: SA-5 Information System Documentation)

We recommend APS define at the highest level an “information security policy” which is approved by management and which sets out the organization’s approach to managing its information security objectives. APS needs to update their program to ensure regular reviews of the information security policies at planned intervals or when significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. All documents should be reviewed and approved by management on at least an annual basis, communicated and conduct training to all relevant parties. These documents should all follow a framework such a Documentation Hierarchy Pyramid to provide control and guidance.

The information security policy should be supported by specific information security areas including, but not limited to:

- | | |
|---|--|
| <input type="checkbox"/> Cloud Computing Policy | <input type="checkbox"/> Incident Response |
| <input type="checkbox"/> Data Loss Prevention Policy | <input type="checkbox"/> Malware Protection Policy |
| <input type="checkbox"/> Patch Management Policy | <input type="checkbox"/> Third-party Oversight |
| <input type="checkbox"/> Disaster Recovery | <input type="checkbox"/> Physical and environmental |
| <input type="checkbox"/> Information Transfer Policy | <input type="checkbox"/> Business Continuity |
| <input type="checkbox"/> Clear-Desk Policy | <input type="checkbox"/> Mobile Device Policy |
| <input type="checkbox"/> Acceptable Use Policy | <input type="checkbox"/> Change Management Policy |
| <input type="checkbox"/> Access Control Policy | <input type="checkbox"/> Security Policy |
| <input type="checkbox"/> Data Classification Policy | <input type="checkbox"/> Cryptographic Controls Policy |
| <input type="checkbox"/> Sensitive Information Policy | |

Management's Response

The APS technology team **partially accepts the recommendation** of the audit finding. As we implement the document repository platform, we will also ensure that documents are updated to reflect recent infrastructure /architecture changes. We, however, do not believe that all the documents recommended have relevance to APS (i.e. Telework Policy).

Anticipated Completion Date

- Implement 'Technology Document Repository' – March 2019
- Complete document review/updates – June 2019

7. Backup and Restore Controls ⬢

During the interview with the Director of Infrastructure, Rausch was informed there are regular backups for critical systems. However, formalized documentation on backup and restores was unable to be provided to Rausch. Rausch learned during the interview with the Oracle DBA and Applications Director, there is an Infor Lawson Financial upgrade in process. In order to perform development and testing, there are Lawson financial restores in the development environment to test systems. No other evidence of backups or restores were able to be provided.

Risk

To protect against loss of data, backup copies of information, software and system images should be taken and tested regularly. Losing data leads to many problems. From an operations standpoint it leads to loss of productivity. From a historical standpoint it means data that has been collected, analyzed, and perfected for years (possibly even decades) can be permanently gone.

Recommendation (NIST: CP-9 Information System Backup)

Rausch recommends a backup procedure should be established to define the organization's requirements for backup of information, software and systems and the process by which this can be accomplished. This procedure needs to be part of the Disaster Recovery Policy.

- I. The backup policy/ procedures should define the retention and protection requirements. Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
- II. When designing a backup plan, the following items should be taken into consideration:
 - a. Accurate and complete records of the backup copies and documented restoration procedures should be produced.
 - b. The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization.
 - c. The backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

- d. Backup information should be given an appropriate level of physical and environmental protection at both the backup and main site locations.
 - e. Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss
 - f. In situations where confidentiality is of importance, backups should be protected using encryption.
- III. Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.
 - IV. Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.
 - V. The retention period for essential business information should be determined, considering any requirement for archive copies to be permanently retained.

Management's Response

While the auditor was not provided with documents related to the backup and restore procedures, this should not be interpreted to mean that they do not exist or that there are no backups being performed. The APS technology team *admits that most of these documents need to be reviewed, updated and included as part of finding # 5 above (Outdated Documentation).*

Anticipated Completion Date - June 2019

8. System Development Life Cycle Controls

Rausch noted Lawson is written in the COBOL language for the application and its customized configurations. Changes to the customized configurations are managed by the APS Lawson development team, with only one member authorized to move changes into production. Currently there are no source code management utilities to help APS manage versioning or source code check-in/out. Rausch noted during the interview there are very few changes made to the customized configuration source code.

Infor Lawson Global Human Resources is currently maintained by RPI, a third-party contractor. Source code is Infor Lawson proprietary JAVA. All changes are monitored and managed by the APS development team. RPI is not allowed to move changes into production. Rausch noted there was no date on the "SDLC methodology" and the "Software Development Life Cycle" was dated Jun 2005. The current environment controls described above are not reflected in these documents.

Risk

System Development Life Cycle (SDLC) process describes a process for planning, creating, testing, and deploying an information system. The controls for the SDLC process can change when the environment the information systems running on change. Updates to the SDLC process and controls should be updated to reduce the occurrence of unauthorized changes.

Recommendation (NIST SA-3 System Development Life Cycle)

Rausch recommends APS update their SDLC process and controls documentation that support the current environment. The updated documentation should define the roles and responsibilities for new development as well as maintenance and enhancement programs for projects. Supporting documentation needs to be captured for each project. Describe the models used (Waterfall or Agile). Describe the governance and oversight for each stage of the process.

Management's Response

APS technology team **partially accepts the recommendation** of the audit finding that the referenced documents should be reviewed, updated and included as part of finding # 5 above (Outdated Documentation). However, APS rarely does software development and will not require the level of rigor typically required for a full SDLC. We will work with the OIC to agree on the acceptable level of documentation required for our unique situation.

Anticipated Completion Date - June 2019

9. Data Center Environmental and Security Controls

Rausch noted there is badge access control to the data center and is managed by the Security Office. The data center environmental and capacity planning is handled by Operations. However, documentation on how the capacity planning for uninterrupted power supply, air-condition and power distribution is performed and if it is included as part of a BIA or risk assessment was unable to be provided. Additionally, Rausch observed quite a few cardboard boxes stored in the computer room during tour and this is considered an environmental and fire hazard to the equipment

Risk

Data centers are limited in terms of footprint, power consumption and cooling capacity. Capacity planning should be included in any holistic risk management plan that involves all aspects of the business. Capacity planning could be limited to your internal network or hosted infrastructure depending on the nature of your distributed infrastructure. In either case, the process is the same. You will need to determine the impact to your business if your network were to have availability issues due to infrastructure limitations. Additionally, cardboard and paper in a data center exposes the equipment to dust contamination and fire risk.

Recommendation (NIST: PE-1 Physical and Environmental Protection Policy and Procedures)

Rausch recommends APS document a data center environmental and capacity planning procedure to chart a capacity plan and determine what strategy will accommodate business needs best. This procedure

should also address the need to maintain a clean data center free of fire hazards and airborne contaminants.

Management's Response

While the IT technology team does not have a copy of the capacity plan from the original heating/cooling assessment conducted a decade ago, it should be noted that the team is utilizing only about 50% of the planned capacity of the data center server room. We believe that the UPS, air-condition and power distribution currently exceeds the needed capacity. The finding concerning the cardboard boxes has been addressed. We will review this finding further with the OIC.

Anticipated Completion Date - June 2019

ADVISORY SERVICE

