Richmond City Council

The Voice of the People. *Richmond, Virginia*

OFFICE OF THE CITY AUDITOR

Audit Report No. 2009-05

on the

Richmond Public Schools
Department of Information Technology

February 2009

OFFICIAL GOVERNMENT REPORT

Richmond City Council

OFFICE OF THE CITY AUDITOR

900 East Broad Street, 8th Floor

Richmond, Virginia 23219

804.646.5616 (tel); 804 646.2230 (fax)

Committed to increasing government efficiency, effectiveness, and accountability on behalf of the Citizens of Richmond.

THIS PAGE LEFT BLANK

INTENTIONALLY

TABLE OF CONTENTS

THIS PAGE LEFT BLANK

INTENTIONALLY

CITY OF RICHMOND
CITY AUDITOR

Executive Summary

February 20, 2009

The Honorable Members of Richmond City Council
The Honorable Members of Richmond Public Schools Board
The Richmond City Audit Committee
Dr. Yvonne Brandon, Superintendent of Richmond Public Schools

Re: Audit of the Richmond Public Schools Department of Information Technology

The City Auditor's Office has completed an operational audit of the Department of Information Technology for the 12 months ended December 31, 2007 for the Richmond Public Schools (RPS). The audit was conducted in accordance with Generally Accepted Government Auditing Standards.

The overall objective of this audit was to review the RPS Department of Information Technology (RPS DIT) operations and to:

- Evaluate the efficiency and effectiveness of operations;
- Verify compliance with policies, procedures and regulations; and
- Determine the existence and effectiveness of internal controls and safeguarding of assets.

Findings

The auditors concluded that the RPS DIT's governance of information technology appears to be weak. Supporting the auditors' conclusion the following was identified:

- RPS DIT does not have a formalized risk assessment process in place. Without such an assessment process, it is impossible to create a risk mitigation plan.
- RPS DIT Disaster Recovery and Business Continuity Plans are outdated, incomplete,

and inadequate. The primary goal of planning for a disaster is to prevent interruption of mission-critical services and to re-establish full system and business functionality as swiftly and smoothly as possible.

- RPS DIT does not have a formal change management process exposing IT resources and information to the vulnerabilities of being altered without proper authorization.
- RPS DIT does not have a formal configuration management process in place and lacks related formalized policies and procedures.

In general, the auditors also concluded that:

- RPS DIT lacks formalized policies and procedures in many IT areas. Many of the critical tasks may not be performed consistently and appropriately. That lack of clear and concise policies could lead to vulnerabilities in security and management of information systems and loss of critical RPS data.

Other salient findings:

- RPS DIT currently lacks a systems development life cycle methodology in order to manage the implementation and modification to systems and applications. Without a structured methodology, changes to the production environment could result in the following risks:
  - User requirements and objectives not being met by the application system;
  - Performance criteria not being met;
  - Employee productivity declines;
  - Insufficient documentation;
  - Inadequate adherence to accepted systems development methodologies; and
  - Insufficient planning for data conversion/migration and cutover and post cut-over disruption to business relevant to a new software implementation.

- RPS' AS/400 computer system holds all of their critical operational, financial and educational information and is the primary system of record. The auditor evaluated the effectiveness of system controls. Out of twenty-two system controls (identified as high or medium risk); seven were not in compliance with industry standards.
- Out of the 19 logical access controls tested, six password settings were not in compliance with relevant best practices. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring user IDs, passwords, or other identifiers that are linked to predetermined access privileges.
- Granting, terminating, updating and maintaining system users within the network environment needs improvement. The manual process used to grant, modify and terminate access does not utilize compensating controls such as an authorized signature list.
- Other than in the payroll module, the application audit trail logging feature of the AS/400 is not actively used. If the records are manipulated, the changes may not be detected. In addition, the identity of the employee making adjustments will not be determined. The audit trail logging feature was purchased but was not turned on due to resource requirements which, if turned on, could jeopardize the efficiency of the system.
- Currently, DIT developers have access to the AS/400 production database and various modules having the ability to implement their changes. This ability may lead to unauthorized, undesirable changes made to an application that may not be detected and corrected in a timely manner.
- RPS does not utilize an intrusion prevention and detection systems nor has it conducted a network security intrusion detection analysis. These systems are essential to enhance the perimeter security of the network by detecting external attacks and blocking penetration of the perimeter firewall. An analysis evaluates the configuration of the external firewall, computer networks, and network configuration of internal infrastructure equipment to detect any weakness.

- Auditors reviewed the wireless configurations of several access points for RPS. It was determined that RPS DIT has adequate controls over its wireless network services. However, the Network Operations Group needs to formally document policies and procedures outlining how wireless access points should be configured. In addition, the Network Operations Group lacks tools to scan the network for unauthorized wireless routers.
- RPS DIT does not have adequate procedures for monitoring the performance of their IT vendors. Without such procedures, it is not possible to assure receiving the proper value for taxpayers' funds entrusted to RPS.
- RPS DIT computer hardware maintenance (maintaining, servicing and performing preventive maintenance) was found to be adequate.
- RPS does not have a definitive list of all of their software licenses. Accordingly, they are not in the position to verify the existence of licenses for all software copies in use. This exposes RPS to possible significant legal liabilities and public embarrassment.
- RPS personnel could not locate 13,455 or 42% of the computer equipment identified through the fixed asset system. It appears that there is a possibility of a significant number of errors in RPS' fixed assets system. However, the possibility of missing equipment cannot be ruled out.
- RPS has purchased an application called LANDesk to track their hardware and software. However, the auditors found that RPS did not purchase an adequate number of licenses for the LANDesk application. Audit inquiries revealed that RPS possesses only 76% of the total licenses needed for this application. Due to the inadequacy of licenses, RPS may not be able to identify all errors in records and missing assets.
- RPS uses a free vendor supported email system. RPS staff noted various concerns about this system's operability. These concerns related to extended downtimes and lost or delayed emails. Deficiencies of this email system are outside the ability of RPS DIT to fix and are the responsibility of the vendor. The backup and recovery

function of the email system lies completely with the service provider. RPS's only course of action is to contact the vendor and report the problem. This appears to be a significant issue as the security and reliability of a communication system is left to a vendor against whom RPS has limited recourse. RPS personnel were not able to provide contract documentation between Richmond Public Schools and the service provider.

- RPS has not yet implemented recommendations made by an outside consultant, communicated in the City Auditor's report dated June 19, 2008, relating to RPS DIT fire suppression, HVAC system, and backup generator security.

The City Auditor's Office wishes to thank the RPS DIT staff for their cooperation during this audit. Subsequently, auditors will evaluate opportunities for consolidating certain IT functions of RPS DIT with that of the City Department of Information Technology. A written management response and action plan to this audit is included in Attachment A. Please contact the City Auditor's Office if you have any questions or comments.

Umesh Dalal, CPA, CIA, CIG
City Auditor

THIS PAGE LEFT BLANK

INTENTIONALLY

Comprehensive List of Recommendations

THIS PAGE LEFT BLANK

INTENTIONALLY

Introduction, Objectives, Methodology and Background

Introduction

The City Auditor's Office has completed an operational audit of Richmond Public Schools Department of Information Technology (RPS DIT) for the 12 months ended December 31, 2007. The audit was conducted in accordance with Generally Accepted Government Auditing Standards.

RPS DIT is tasked with the responsibility to ensure secure and reliable access to data for the Richmond Public School system. This requires maintaining a system of internal controls over their IT environment. In fulfilling this responsibility, management is required to assess the expected benefits and related costs of the control procedures. The audit procedures utilized in this audit provided a reasonable basis for concluding that overall, RPS DIT internal controls need significant improvement.

Due to the magnitude of the various applications and processes, and in conjunction with the lack of previous audit coverage, a more comprehensive audit of each functional area will need to be conducted at a later date.

Objectives

The overall objective of the audit is to review RPS DIT operations in order to:

- Evaluate the efficiency and effectiveness of operations;
- Verify compliance with policies, procedures and regulations; and
- Determine the existence and effectiveness of internal controls and safeguarding of assets.

Methodology

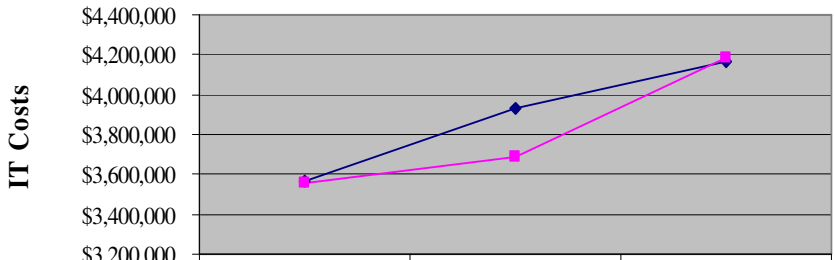
Auditors performed the following procedures to complete this audit:

- Interviewed management and staff;
- Surveyed management and staff using questionnaires;
- Reviewed and evaluated relevant policies and procedures;
- Reviewed financial data, supporting documents, data flows, and diagrams;
- Observed and tested various IT system controls;
- Reviewed and evaluated network infrastructure;
- Reviewed prior IT related audits and previous relevant consultant reports; and
- Conducted other appropriate tests as deemed necessary.

Background

Information Technology plays an important role in RPS' administration, operations and educational services. Over the years, the funding for this function has increased gradually as depicted in the following graph:

Trend of School DIT Costs



	2005	2006	2007
Budgeted	$3,567,818	$3,928,658	$4,165,061
Actual	$3,560,520	$3,684,506	$4,183,241

Richmond Public Schools has undergone various audits and reviews over the recent years. In 2007, the School Board agreed to have the City Auditor's Office conduct an audit of RPS DIT to evaluate the feasibility of consolidation of services with the City's Department of Information Technology. Accordingly, this audit was conducted. This report presents the salient results of the audit. The feasibility of consolidation of the Departments of Information Technology for RPS and the City will be studied at a later date and the results will be reported upon completion of the study.

Areas Analyzed

This audit is divided into the following:

- Governance of the IT Infrastructure and Processes
- Internal Controls Structure
- Asset and Contract Management
- Staffing
- Follow-up on IT audit recommendations in the previous report issued in June, 2007

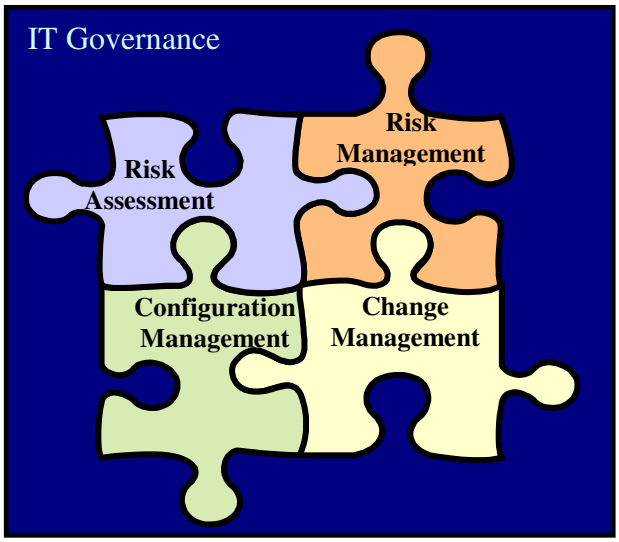
Governance

Introduction

IT governance helps in the management of IT systems and infrastructure within accepted risk parameters

Much of RPS DIT's operation depends upon well functioning information systems. Therefore, proper governance of the overall IT environment is critical for the success of RPS operations. IT governance provides a structure to manage and use information systems and infrastructure within accepted risk parameters. There are several separate components of this process to make sure that proper procedures exist to carry out operations, and risks are managed to prevent disruptions and to safeguard data. This process involves risk assessment, mitigation, and monitoring of residual risks, if they exist.

IT governance includes the following components:



IT governance is neither complete nor effective if any of the above components are lacking.

Risk Assessment

Risk assessment identifies and assesses factors that may prevent a system, application, process or project from achieving their respective business goals. In other words, risk assessment helps the organization develop processes to manage their system flawlessly and avoid unnecessary interruptions. This also prevents adverse impact on organizational productivity due to information system failures.

RPS has not formally assessed organizational IT risks

Upon inquiries, auditors identified that RPS DIT does not have a formal risk assessment process and, accordingly, organizational IT risks are not assessed. Without such assessment it is impossible to create a risk mitigation plan. In this situation, any major interruption of the computer system may disrupt classroom education or the administration of school activities.

Recommendations:

1. ***Conduct an organization-wide IT risk assessment and compile a formal mitigation plan.***

2. ***Periodically, evaluate the relevance and adequacy of the risk assessment and the formal mitigation plan.***

Risk Management

Proper risk management prevents and mitigates system interruptions

Risk management addresses vulnerabilities and threats to the information system resources identified by the risk assessment. This process, if conducted effectively, will limit risk to an acceptable level. It requires significant planning to mitigate potential threats to the IT environment and ensure the organization's ability to continue business during and after a major disaster. The primary goal of risk management is to prevent interruption of mission-critical services and to re-establish full system and business functionality as swiftly and smoothly as possible. It is important that these plans are clearly

documented, properly communicated, updated, and regularly tested. The following section describes the necessary planning RPS must have.

A. Disaster Recovery Planning:

A disaster recovery plan includes a set of procedures to ensure that essential components such as networks, infrastructure, applications, and data can be restored after a major interruption such as fire or natural calamities. This planning is very critical as it is necessary to resume RPS operations and educational services soon after the disruption occurs.

RPS' Disaster Recovery Plan is seriously outdated

Auditors observed that the disaster recovery plan provided by RPS DIT was seriously outdated. The plan included the same content and sections as the original outdated version dated September 17, 2003. The latest version of their disaster recovery plan still listed former employees as key contact individuals. Contrary to generally accepted best practices, based on the available documentation, this plan has never been tested to determine its relevance and functionality.

Generally, during a major disruption, the primary facility may become dysfunctional and unable to continue providing IT services. It is a common practice to have a third-party agreement that provides for a recovery facility, computing, and telecommunications that can be used during and immediately after a disaster until the primary facility operations can be restored. Other options include:

- A reciprocal agreement with another school district to provide disaster recovery resources.

- A cold site that provides only the facility without the hardware, software and other IT related resources.
- A warm site that provides the facility and a minimal amount of hardware and software and other IT related resources
- A hot site that provides the facility, hardware, software and other required IT related resources.

RPS does not have the means to restore operations after a major disaster

RPS would need to conduct a cost benefit analysis to determine the type of disaster recovery site that meets their business needs.

Not having a facility to restore operations could delay resuming RPS' business significantly, which may have an adverse impact on educational services. Generally, an agreement with a third party for the use of its facility in the event of a disaster is a very cost effective solution for organizations like RPS. It appears that the current situation warrants immediate attention to mitigate risks during and after disasters.

B. Business Continuity Planning:

Business continuity planning is a logistical plan for recovery and partial or complete restoration of interrupted mission-critical systems, processes or environments, within a predetermined time. It includes a business impact analysis to develop strategies for minimizing risk and identifying the impact of disruptions. Generally accepted best practices, COBIT (Control Objectives for Information Related Technology), recommend that IT continuity plans be designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding and potential business impacts and address

requirements for resilience and alternative processing of all critical IT services. It should also cover usage guidelines, roles and responsibilities, procedures, and communication processes. Also, the business continuity plan has not been tested on a regular basis.

RPS's business continuity plan is inadequate

RPS DIT has a business continuity plan (BCP) dated November 12, 2004. However, it was poorly organized and consisted of various articles and internet excerpts from other BCP models instead of being written specifically for RPS. Also, RPS DIT has not performed a business impact analysis on their current mission-critical systems and applications.

Not performing such an analysis severely hinders DIT from developing and selecting a business continuation strategy. In this situation, RPS' IT management may not be able to keep system mission-critical processes operational in the event of a disruption. Auditors were informed that DIT is in the process of updating their disaster recovery plan and business continuity plan.

Recommendations:

3. ***Create disaster recovery and business continuity plans in accordance with generally accepted best practices such as the COBIT framework, to reduce the impact of a major disruption on key business functions and processes.***

4. ***Test the disaster recovery and business continuity plans on a regular basis.***

5. ***Provide all staff with regular continuity planning training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Modify the training as necessary based on the test results.***

6. ***Develop a disaster recovery solution to provide an appropriate computer facility to resume RPS' business during and after disasters.***

7. ***Create an effective process for monitoring the vendor providing the disaster recovery facility by clearly defining the roles, responsibilities, expectations, service levels and performance indicators.***

Change Management

Change management is a process of systematically dealing with system changes

Similar to any other processes, Information Systems are constantly updated and subjected to changes. Change management is a process of systematically dealing with changes. The goal of the change management process is to utilize standardized methods, procedures, and tools for the efficient and prompt handling of all change requests. A formal change management process ensures that all parties impacted by a change have been properly notified, risk associated with the change has been properly assessed, and backup and recovery processes are in place if the change process fails.

Also, if changes are not properly updated, existing system documentation may become unusable and create confusion related to the system's functionality. Any future changes that are in conflict with the undocumented changes may impact system performance.

Therefore, a formal change management process is essential to reduce or eliminate disruptions in business activities.

The elements to consider in a change management process include:

- Identification of changes
- Categorization
- Prioritization
- Emergency procedures

- Impact assessment
- Change authorization
- Release management

Care must be exercised that only authorized and valid changes are made to the system. The lack of a proper change management policy results in the following risks:

- Unauthorized or unplanned changes could be applied to the production environment. RPS DIT personnel may be unable to track all changes back to a documented change request authorization resulting in weak accountability for production changes.
- Confusion may result due to the inability to determine the nature and extent of changes made to applications.
- Changes may contain errors which could disrupt systems.
- RPS DIT may not be able to restore the previous baseline or fix problems with the implementation.

COBIT best practices recommend that all changes, including emergency maintenance and updates relating to infrastructure and applications, must be formally managed in a controlled manner. Changes to procedures, processes, systems and service parameters need to be logged, assessed and authorized prior to implementation. They must be reviewed against planned outcomes following implementation. This assures the stability and integrity of the production environment.

RPS does not have a change management policy

Contrary to recognized practices, RPS DIT does not have a change management policy. This is a very critical deficiency in IT governance at RPS.

Due to the lack of documentation, auditors could not verify that RPS DIT personnel consistently made only authorized changes to the systems and network. It is imperative that RPS DIT changes are scrutinized and approved prior to adopting them. There is a need for establishing appropriate procedures for these purposes.

Traditionally, for a large organization such as RPS, a Change Advisory Board (CAB) is appointed. This is an authoritative and representative group of people responsible for assessing, from both a business and a technical viewpoint, all significant (high-impact, high-risk) change requests. Currently, RPS does not have such a mechanism.

Recommendations:

8. ***In accordance with industry best practices, create appropriate policies, standards and procedures that clearly outline the change management process.***

9. ***Create a Change Advisory Board or similar mechanism and describe pertinent roles and responsibilities for personnel involved.***

10. ***Require the Change Advisory Board or similar group to review and approve all change requests and related metrics based on established change management policies, standards, processes and procedures.***

11. ***Educate users and IT professionals about processes and procedures related to requesting and implementing system changes.***

Configuration Management

Configuration management involves describing an organization's computer systems including all hardware and software components. This information typically includes versions and updates that have been

applied to installed software packages and the locations and network addresses of hardware devices. During this audit, RPS DIT used specialized software that provided a list of the network configuration equipment. Typically, this type of application is used to maintain network equipment.

Auditors' review of reports from this application confirmed RPS' compliance with the following:

Generally Accepted Practices	DIT in compliance
System/network architectures should be documented, maintained on file, and updated when needed.	**Yes**
Detailed information about all devices connected to the network should be captured in the configuration listing, including device names, network addresses, installed application components, system software products and versions, etc.	**Yes**
Configuration information should be kept up to date when new changes are implemented or new devices installed. Periodic inventories should be performed to validate the accuracy and completeness of the configuration listing.	**Yes**
Configuration listings should be used to help maintain standardization and consistency. It identifies dependencies for changes (e.g., what applications will be impacted due to a change) as well as to handle software updates and patch management.	**Yes**
Ensuring the integrity of hardware and software configurations includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed.	**Yes**

It was not possible to verify if RPS is following their undocumented configuration management practices in a consistent manner

RPS DIT personnel indicated that they do not have formal configuration management policies, processes or procedures in place; however, they are working on creating them. Presently, a tool called Soft Landing is being implemented to address the need for system application change request and configuration management. As this application was not implemented at the time of the review, a detailed analysis was not conducted.

Although RPS DIT is following some of the industry's generally accepted practices, their informal configuration management process is unstructured, rudimentary and conceivably prone to error. It does not include all necessary components of configuration management. There is no way to verify that the informal practice is consistently followed. Also, RPS DIT will need a centralized configuration management database (CMDB) application or other centralized configuration management tool in addition to a formal configuration management policy.

A CMDB is a repository of information related to all the components of an information system. A key goal of a CMDB is to help an organization understand the relationships between these components and track their configuration.

Effective configuration management facilitates greater system availability, minimizes production delays and resolves issues more quickly. In addition, a lack of these procedures could result in:

- Employees using their own software or secondary data storage devices that may increase the risk of introducing viruses and malware to RPS systems; and

- An increase in non-compliance with RPS' IT policies and procedures.

Recommendation:

12. Establish a formal configuration management policy in accordance with best practices such as COBIT and implement proper procedures and supporting tools to comply with the policy.

Internal Controls

This section of the report will discuss the issues related to internal controls that impact IT governance, RPS operations and the overall IT environment. Since there are multiple control issues presented, audit observations are organized in the following categories:

- Policies and procedures
    - IT Control Environment & Information Security Management
    - Network Security Infrastructure
        - Security Awareness
        - Incident Handling
    - Systems, Applications & Operations
    - Web-based Applications Operational Infrastructure
    - Data and Database Security
    - Data Backup Process
    - IT Service Desk
- Systems Development
- System Controls
- Logical Access Controls
- Segregation of Duties
- Network Architecture and Infrastructure Configurations
- Wireless Technology Security Infrastructure
- Active Directory

Policies and Procedures

Documented, formal policies and procedures are an essential part of the governance process. Policies are high-level documents that represent RPS DIT's corporate philosophy and strategic thinking of senior management. Policies reflect management's guidance and

direction in developing controls over information systems and related resources.

Procedures are detailed steps needed in order to comply with the policies. Without formal, written procedures, organizational policies may not be complied with consistently. According to the FISCAM (Federal Information Systems Controls Audit Manual), "The IT control environment policies and procedures should set the tone of an organization, influencing the control consciousness of its people. It should be the foundation for all other components of internal control, providing discipline and structure."

Auditors evaluated DIT policies and procedures in various areas and the results are discussed as follows:

1. <u>IT Control Environment and Information Security Management</u>

The IT control environment encompasses the architectural standardization that includes formal policies, procedures and standards. RPS uses a computer operating system known as AS/400 and its control environment architecture is designed to work with this operating system. All supporting applications interface with the AS/400. RPS has policies and procedures that address the overall system security controls of the IT environment. However, based on the available documentation, it is not clear if the policies and procedures are periodically reviewed and updated if applicable. Also, the existing policy does not accurately reflect security changes made to the AS/400 operating system. Ongoing reviews are necessary to keep procedures updated and relevant.

It is not clear if the policies and procedures are periodically reviewed and updated

Effective security management is intended to maintain the integrity of information and protect IT assets while minimizing the business impact of security vulnerabilities and infractions. It includes establishing and maintaining security roles and responsibilities, policies, and procedures. DIT senior staff is currently in the process of revising these policies and procedures to align them with current IT practices, along with the new vision and mission of the reorganized IT department.

When security policies and procedures do not accurately reflect management's vision, the following weaknesses are probable:

- Policies may not exist, may not be kept current, and/or may not be documented in an easily understandable format.
- There could be no accountability relative to inappropriate employee behavior.
- Unsafe business practices could lead to an internal data breach (e.g. users not securing passwords such as writing them down on "sticky" notes).

Recommendation:

13. Update policies and procedures addressing overall IT control environment security concerns.

2. <u>Network Security Infrastructure</u>

Network security policies and procedures include establishing and maintaining network security roles and responsibilities, standards, and tools. Network security management also includes performing

security monitoring, periodic testing, and implementing corrective actions for identified security weaknesses or incidents of breach.

Lack of up-to-date network security policies and procedures results in control weaknesses

Lack of up-to-date network security policies and procedures results in the following weaknesses at RPS:

- The network administrators are left to determine the security settings without guidance and management's input.
- Network changes may not be effectively communicated to upper management in a timely fashion.
- Expectations of network staff may not be properly communicated.
- RPS network users may not understand or comply with control requirements and upper management's expectations about network security.
- Weakness in internal controls (and areas of excessive risk) may not be identified by management or given priority for correction

The auditors' review indicated that RPS utilizes network applications adequately. They have documentation for network management such as network schematics and configuration files for network equipment. However, the governing policy that guides the management of such devices is nonexistent.

Recommendation:

14. Create network security policies and procedures based on a risk analysis, best practices, and management's revised mission and vision. The new policies and procedures must include version control, training, and a communication plan.

2.1 Security Awareness

Currently RPS does not have a security awareness program that informs users of RPS DIT security expectations. RPS DIT does not have formal policies that outline acceptable use such as an Internet policy. They provide initial new-hire security training, however no on-going security awareness training is provided.

Generally accepted practices for establishing and maintaining security awareness include:

- Informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality;
- Distributing documentation describing security policies, procedures, and individual responsibilities, including user conduct;
- Requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security, including the consequences of security violations, and their responsibilities for following all organizational policies, including maintaining confidentiality of passwords and physical security over their assigned areas; and
- Requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.

Recommendations:

15. Implement a security awareness program to inform users of RPS DIT security expectations. A signed security form must be created and retained by RPS DIT to ensure staff is held accountable for security awareness.

16. Create an annual training plan to ensure that security standards are reinforced.

2.2 Incident Handling

When an organization's network has been compromised, an incident response process is necessary to address the breach. It is the responsibility of the IT department to respond to the problem effectively and quickly. Therefore, a formalized process that includes policies and procedures must be created.

According to FISCAM, "The two main benefits of an incident handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage. For example, the use of virus identification software is an important tool to help contain damage from viruses."

Without an incident response policy and staff trained in incident response, the organization is at greater risk of:

- Improperly handling and documenting an incident;
- Inadequate internal communication and organization preparedness, and
- Tainting the ability to pursue prosecution of a network offender by improper information gathering and documentation of an incident.

RPS staff does not have policies, processes and procedures to handle a network security breach

If a network incident were to occur, the staff does not have standard policies, processes and procedures needed to respond to an incident. The risk of loss of information or the inability to continue RPS' daily operations is beyond acceptable tolerance levels. This discrepancy could result in compromising confidential student records.

Recommendation:

17. Create incident response policies and processes to ensure that all incident responses are handled efficiently and effectively.

3. **Systems, Applications and Operations**

DIT has several critical operating systems and applications. The AS/400 maintains the core information infrastructure. RPS also utilizes many web based applications. Some web based applications interface with the data stored on the AS/400, while other web based applications are stand alone applications.

The development staff use IBM user guides for the operation of the AS/400, but no formal policy exists to ensure that the developers work on the AS/400 operating systems in a consistent manner.

Recommendation:

18. Create AS/400 systems operations and applications policies and procedures based on industry best practices. To ensure adherence to the new policies, a communication and training plan must be implemented.

4. Web-based Applications Operational Infrastructure

Web applications allow organizations to effectively process information and are compatible with many different applications, making the applications easier to build and maintain over time. These applications are accessed via a web browser over a network such as the Internet or an Intranet. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their increased use.

The access security for the web applications is controlled through a web portal that grants access by a network application. Access to the individual web applications are determined by the individual's user profile on the AS/400. The network portal grants access to the web applications that interface with the AS/400. The security controls are centrally maintained within the AS/400 applications. The portal does not store any information on the client machines and all changes are stored directly on the AS/400.

Auditors reviewed the logical placement of the web servers on the network diagram while conducting the audit test work. The RPS web applications are separated from the internal network and are stored on the web servers. The logging file folder for the websites is properly secured. The logical design of the web servers was reviewed with the Server Group and file permission and controls were reviewed at the console. The file permissions and access were adequate.

The infrastructure setup for web-based applications was found to be adequate

The RPS DIT website is located outside of the perimeter firewall. All web applications can only be accessed through the DIT website. All stored data for the web applications are stored on databases inside the network. The web applications are the intermediary between the user and the database. The end users have access to the web application but not to the database. The web application retrieves and updates the database based on the user's rights (security settings). Based on the results of the audit test work, the infrastructure setup for web-based applications was found to be adequate.

RPS DIT does not have formally documented procedures to create and maintain web applications

Auditors reviewed the web applications' security parameters and noted RPS DIT does not have formally documented policies and procedures for the web developers to create and maintain web applications. However, the Web Development Group uses web applications' tools with security features to update and maintain their web applications and the RPS web pages. RPS DIT needs to develop operational standards and security guidelines for securing, creating, and updating web applications.

Recommendation:

19. ***Establish operational standards and security guidelines for securing, creating and updating web applications.***

5. Data and Database Security

The organizational data represents a very valuable asset for RPS. Databases are organized repositories for data that assure the reliability of data in a multi-user environment. Data access services within a database are provided by a system layer called a Database Management System (DBMS). The primary objective of the

database is to enable multiple users to access a single data repository while maintaining data reliability and integrity. The secondary objective for the database is to provide security services for the data stored within the database.

RPS uses DB2 database structure that does not allow access to a user if another user is in the process of modifying data. This setting helps to ensure that the data is reliable and conforms to database standards. The auditors validated this process through observation.

To achieve integrity, transactions must meet certain criteria. The data tested on the DB2 database appropriately meets requirements for integrity by having the individual transactions being atomic, consistent, isolated and durable as defined in the following table:

Generally Accepted Practices	DIT in compliance
Atomic -A transaction should represent an indivisible unit of work. All of its actions should succeed or fail together. • Components of a "unit of work" must be compiled together within the boundaries of a single transaction.	**Yes**
Consistent - A transaction must be able to attain a stable and reliable result. If the transaction cannot achieve a stable end state, it should return to the system to the original state (e.g. “rollback”). • Transactions should either commit or rollback based on status.	**Yes**
Isolated - A transaction’s behavior should not be affected by other transactions that exclude concurrently. • Locking should be used to isolate one transaction from another.	**Yes**

Durable - A transaction's effects should be permanent after it commits. Committed changes should survive system failures. • Committed changes should be captured in transaction logs and stored on disk regularly to enable recovery in the event of a system failure.	**Yes**

Although DIT is following the generally accepted practices for database security, they still need formal policies

Although DIT is following the generally accepted practices for data transactional security, formal policies and procedures are not maintained.

Recommendation:

20. Create policies and procedures for the DB2 databases security and operational settings of the AS/400.

6. Data Backup Process

Data backup monitoring is performed by a special application

Currently, DIT has a data backup schedule that outlines the backup process. Within the data backup schedule are descriptive procedures. Monitoring is performed using their backup application on a daily basis. This process was observed and includes the staff checking the previous night's backup report to look for any errors. When a backup tape becomes corrupt, the Server Operations staff removes the corrupt tape from circulation.

The current backup architecture for DIT is maintained by a backup application, which is an enterprise level backup and recovery suite. It provides cross-platform backup functionality to a large variety of operating systems. System administrators are not required to document what was backed up and whether the backup was successful or not. RPS does not have a history of when individual

files or databases are backed-up. Without a history of backups, RPS is unable to verify the validity and reliability of the back-up process.

Some of the generally accepted practices for data backup and retention include:

Generally Accepted Practices	DIT's compliance
All directories (at least the production directories) should be backed-up.	**Yes**
Both on-site and off-site copies of tapes should be created.	**Yes**
Tapes should be stored in a secured and physically protected site.	**Yes**
Library management software should be used to track the files that are stored on tape volumes, as well as the retention and location of the tapes.	**Yes**
Data should be backed-up on a scheduled frequency	**Yes**
A monitoring process should identify any errors in the backup process so that alternate backup tapes can be created as needed	**Yes**

Although DIT is following the generally accepted practices for data backup, formal policies and procedures are not documented. Without formal documentation it may not be possible to assure completeness of the back up process.

Recommendations:

21. ***Create a formal set of policies to address data management. Include the development and execution of architectures, standards, practices and procedures that outline the full data lifecycle in accordance with best practices and management's new vision. The updated data management policies and procedures must include revision and review dates.***

22. ***Implement a communication and training plan to ensure adherence to the new policies.***

23. ***Create a formal process of recording all successful and unsuccessful backups to document the validity and the reliability of the backup process.***

7. IT Service Desk

The Service Desk proactively keeps users informed of all relevant service events, actions and service changes that are likely to affect them. The RPS policies and procedures provide a generalized framework for the Service Desk function. As part of the DIT departmental reorganization, the Service Desk function is in the process of being reengineered and improved by adding service desk monitoring software applications and tools, creating policies and procedures, and increasing their staffing.

Currently the Service Desk is using a helpdesk tracking software to track all service tickets. This process is still in its infancy and RPS DIT has not fully developed a formal process to prioritize its service tickets. A diagnostic analysis and reporting function for the Service Desk has not been formalized. The Service Desk personnel have been given the ability to assist end users by utilizing specialized software called LANDesk and password reset capabilities.

The current procedures do not include performance measures for the Service Desk

The tracking of help desk tickets and the utilization of LANDesk were found to be adequate for the Service Desk environment. However, the current procedures do not include performance measures for the Service Desk staff. Without proper measures, performance of this function cannot be evaluated.

Risks related to inadequate performance of the Service Desk function are:

- System management issues may arise
  - Systems may not be available when needed
  - Significant host and communication problems might go unnoticed
  - Problem indicators might get overlooked
- Problems might not be resolved timely
  - Unscheduled system downtime might cause mission critical applications to be unavailable
  - Appropriate individuals might not be available when needed
- End user's personal computers might remain inoperative longer than an agreed upon threshold
  - Business area management might not be aware of the agreed upon recovery thresholds
  - Extended down times might lead to financial losses for particular systems or applications
- System to fix problem might not function as intended
  - Changes might not fix the problem at hand, and might lead to even more problems
  - Undocumented changes might get eradicated during scheduled upgrades
- Hardware might cease to operate correctly
  - A machine that is not properly maintained is more likely to operate erratically if at all

Recommendations:

24. Create detailed policies and procedures for the Service Desk outlining the processes and expectations of Service Desk personnel.

25. Identify, create, and monitor meaningful metrics to develop baseline standards and expectations of the Service Desk.

Systems Development

The System Development Life Cycle (SDLC) is a structured process by which IT personnel and end users develop, test, implement, and maintain systems and applications. The purpose of an SDLC is to ensure that a consistent, repeatable approach is applied to the development and maintenance process, whereby reducing the risks associated with shortcuts and mistakes.

DIT does not have an SDLC methodology in place to manage the implementation and modification of systems and applications

DIT currently does not have an SDLC methodology in place to manage the implementation and modification of systems and applications. The RPS DIT Server Group is currently modifying its database procedures to incorporate Systems Development Life Cycle methodologies. According to FISCAM, "The Systems Development Life Cycle methodology should provide a structured approach consistent with generally accepted concepts and practices. This approach should include active user involvement throughout the process, is sufficiently documented to provide guidance to staff with varying levels of skill and experience, provides a means of controlling changes in requirements that occur over the system's life, and includes documentation requirements."

In March 2008, a consultant hired by RPS began creating an Application and Database Lifecycle policy, which is pending

completion. These policies and procedures, once completed, should be reviewed and updated by DIT on a regular basis.

Without a structured methodology, changes to the production environment could result in the following risks:

- User requirements and objectives not being met by the application system
- Performance criteria not being met
- Employee productivity declines
- Insufficient documentation
- Inadequate adherence to accepted systems development methodologies
- Insufficient planning for data conversion/migration and cutover and post cut-over disruption to business relevant to a new software implementation

Recommendation:

26. Implement a comprehensive and effective System Development Life Cycle methodology that clearly defines the roles and expectations of the IT staff responsible for implementing, changing, testing and maintaining systems and applications.

System Controls

System controls are designed to mange and mitigate risk within applications systems. System controls are the safeguards that protect the integrity of business application processing.

Seven of 22 controls tested were not in compliance with industry standards

RPS's AS/400 computer system holds all of their critical operational, financial and educational information and is the primary system of record. The auditor evaluated the effectiveness of system controls. Out of the twenty-two system controls evaluated against recommended

IBM settings published in Powertech's Security System Values and benchmarking standards published by ISACA (Information Systems Audit and Control Association), seven of the system controls identified as either a high or medium risk were not in compliance with industry standards. Management recently changed two system controls that were not in compliance with industry standards after being detected by the auditor. The five system controls that are still not in compliance with industry standards are depicted in the following table:

#	Description	Risk per IBM	Complies with		Risk
			AS/400	ISACA	
1	Auditing control	**High**	**NO**	**NO**	The Auditing function is not set to capture critical events. This prevents RPS from being able to see, and manage, what's really happening on the system.
2	Create default public authority	**High**	**NO**	**NO**	The current setting provides too much authority to end-users that have too many AS/400 objects such as libraries, programs, display files and printer files. And, in some instances, the authority is too limited for certain database files that may get cleared and/or deleted as a matter of course. Regardless of the setting at the system value level, the system settings for individual libraries should be used as the primary means of controlling user's authority.
3	Inactive job time-out	**High**	**NO**	**NO**	Leaving a terminal unattended for too long a period of time can expose application programs and system functions to intrusion and abuse by others in the work area.

4	Allow user domain objects in libraries	**Medium**	**NO**	**NO**	Some Vendor Packages may create user Spaces, Indexes, or Queue's in their own libraries. Check with Vendors or monitor the value in the audit logs to determine if access to vendor package libraries should also be named.
5	Verify object on restore	**Medium**	**NO**	**NO**	There is no verification of the legitimacy of objects and exposes the system to potential malicious objects on restore.

RPS DIT must create a baseline of configuration settings that adequately protect the operating system.

Recommendations:

27. Establish a system security baseline for the AS/400. Require the system control values of the AS/400 to comply with industry (IBM and ISACA) benchmark settings.

28. If essential application software requirements prevent benchmark settings from being used, establish compensating controls.

Logical Access Controls

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. The primary goal of logical access control security is to protect business application resources from being accessed by unauthorized methods and to ensure proper segregation of duties. This is achieved by allowing the user just enough system privileges so that their effectiveness in doing their job is not compromised. To ensure appropriateness of user access, a structured process of granting and removing access is needed. Logical security controls enable the entity to:

- Identify individual users or computers that are authorized access to computer networks, data, and resources,
- Restrict access to specific sets of data or resources,
- Produce and analyze audit trails of system and user activity, and
- Take defensive measures against intrusion.

Of the 19 access controls tested, six were not compliant with relevant best practices

The logical access controls assure that the access granted to the AS/400 environment is properly controlled through the system controls. The system controls were tested against industry best practices. Out of the 19 logical access controls tested, six password parameters were not compliant with relevant best practices. After being detected by the auditor, management changed five of the six password parameters, strengthening the login security of the logical access controls. The non-compliant sixth password parameter did not impact the RPS user environment and in the auditor's opinion, the current setting did not weaken the overall password parameters.

The password authorization process needs to be tightened

The process that RPS DIT uses for granting, terminating, updating and maintaining system users within the network environment is initiated by a written request from a supervisor. The request can be in the form of a fax or email, but it has to come from the supervisor. Auditors reviewed copies of emails and faxes to verify compliance with the authorization process. The manual process used to grant, modify and terminate access does not utilize a compensating control like an authorized signature list or automated workflow process. The use of emails or faxes does not guarantee that the supervisor authorized the request because email addresses and faxes can be compromised.

In order to test the effectiveness of this control process, auditors compared the listing of active user accounts against a listing of inactive users. A listing of the 765 terminated employees from the dates of January 1, 2007 to December 31, 2007 was compared to the AS/400 user profile listing. None of the terminated employees from the previous year had active accounts. In addition to reviewing the listing of active and disabled accounts, the notification process of terminating employees was reviewed. However, as noted previously, the auditor could not verify the length of time that it took to delete a user's security profile from the system once the termination was approved because the user's security profile had been deleted from the system. Delayed removal of a terminated employee could result in unauthorized access and a threat to RPS systems.

Audit observations helped management to strengthen the password resetting process

The process for resetting user passwords within the AS/400 environment was reviewed. After proper user verification, the Help Desk resets the user password to a temporary password that must be changed upon the next login. This password reset process created a weak temporary password that was easily guessable. When this risk was brought to the attention of management, DIT changed the AS/400 reset password parameters to a more secure temporary password. After logging on with the temporary password, users are required to create a new password based on strong password parameters for the AS/400 system. The new process appears to be adequate.

The process of ensuring that users have the correct logical access to various records in the AS/400 operating system was also reviewed. The Comprehensive Information Management System (CIMS) Profile Audit Journal File is used to determine what objects are accessed by

users. This journal does not record what the user did, but provides information about what the user accessed.

Payroll is the only module that RPS is using which utilizes a logging feature or process for tracking all changes to the file**.** This is a manual verification process that uses a system generated report called the Payroll Change Report. According to RPS systems personnel, all other modules in CIMS are not utilizing audit trail logging features. The audit trail logging feature allows DIT to review transactional changes made by users in the AS/400 system. The audit trail logging feature was purchased but was not turned on because the previous management determined that there would be insufficient storage resources to track this information. In this case, if the records are manipulated, the changes will not be detected. In addition, the identity of the employee making adjustments will not be determined. The cost-benefit of and the impact of using the audit trail feature must be evaluated.

Not using the audit trail feature may prevent detection of unauthorized system manipulations

Another example of an inefficient audit trail process was found during the current RPS Grants Management Audit where a discrepancy in the electronic data versus the check copy was noted. The payee name from the audit query differed from the vendor name printed on the face of the check. The current process for recording historical data of the check payment history is unreliable. This process does not allow for an accurate and reliable audit trail if the vendor name is changed in the system.

An audit trail control should be in place that would maintain all previous and current vendor names associated with a particular vendor number. If that is not possible, an audit trail feature should be in place

to historically track changes. This would reduce the risk of fraudulent activities and possible duplicate payments to the same vendor with different names.

Many risks are inherent without an audit trail function

With weak processes and without logical access and audit trail logging control settings, there is a greater chance of:

- Security systems being bypassed or turned off;
- Users masquerading on the system as other users;
- Sensitive privileges being abused to compromise security;
- Unauthorized changes made to system software, modules, or applications;
- Security violations and other activities not being logged, tracked and addressed;
- Users not being held accountable for their actions;
- Security control breakdowns not being realized or fixed; or
- Unauthorized changes to system settings going unnoticed, weakening the security of the system.

The above risks appear to be significant and must be addressed.

Recommendations:

29. Assess the feasibility of turning on the audit trail feature to provide the ability to review audit logs ensuring proper system tracking and accountability.

30. Require managers to have a signed access change form for all system access changes. The manager's signature should be verified against an authorized signature list for granting, changing and terminating access.

31. Discontinue email as a method of requesting changes in access privileges. Discontinue the use of faxed requests until an authorized signature list is put in effect. Use an alternative

appropriate mechanism to request and approve changes in access privileges. Evaluate cost benefits of implementing an automated workflow solution.

32. Implement system application controls that will maintain an accurate and reliable audit trail for previous and current vendor checks. If system controls cannot be applied, implement compensating controls to provide the historical audit trail to track previous vendor payments.

Segregation of Duties

Segregation of duties is a standard control procedure

Segregation of duties is a standard control procedure that prevents an individual from conducting all aspects of a transaction without proper checks and balances. IT applications do not leave a visible trail of changes made to the system unless appropriate control procedures and tools are implemented. Therefore, allowing an individual the ability to perform incompatible functions could yield undesirable results that may not be detected and corrected in a timely manner. In the IT environment, development, installation, and access to the production environment should be separated in order to minimize the ability to initiate, perpetuate and conceal a wrongful change to the production environment. With segregation of duties, the risk of impropriety is minimized.

Currently, RPS DIT developers have access to the AS/400 production database and various modules. The developers are currently tasked with making changes to the production environment when they receive requests from users. This is standard practice for the DIT AS/400 Development Group. The developers should not have the ability to implement their changes into the production environment as unauthorized, undesirable changes made to an application may not be detected and corrected in a timely manner.

In this situation, security risks of not properly segregating duties include the following:

- Invalid or fraudulent transactions may be processed.
- Sensitive transactions may not adequately be controlled.
- Users may be assigned excessive or unauthorized access to transactions.
- Security violations or critical processes may not be logged leading to wrongful acts of users.
- Developers may be able to grant more access to themselves without management's knowledge.
- Production data may be inadvertently changed by developers.

The above list represents significant potential control weaknesses and must be addressed expediently.

Recommendation:

33. Require programmers to make all changes in the test environment. Require a different staff member to test all changes prior to making the approved changes to the production environment.

Network Architecture and Infrastructure Configurations

A computer network is a combination of hardware and software. Network architectures are designed to provide standards for enabling computers and other devices to establish communications links, transferring information without conflict, and to control and restrict network traffic from unauthorized access. In order to establish communications and ensure the reliable transfer of information between various components of the computer network, functional layers, interfaces, and protocols (rules) are used. Edge routers and firewalls are key hardware and software devices used to assist in this process.

An edge router is a device that routes data packets between one or more local area networks and can be utilized as the first line of security defense. When an edge router is used in conjunction with a perimeter firewall, the overall security of the network is enhanced. Security firewalls are network devices used to control and restrict network traffic that is allowed to flow between networks, and used to isolate one network from another such as between an organization and the Internet.

Basic network access controls were adequate and functioning

RPS' Network Services Group secures the network environment by removing all services unnecessary for business needs, thus reducing external vulnerabilities. Auditors reviewed the configuration and access to the edge router and firewall. Auditors found that basic network access controls were adequate and functioning. However, further testing may be necessary to obtain a higher level of assurance.

The auditors found that the logical and physical access to the edge router and perimeter firewall are adequately protected within the network environment. The edge router and perimeter firewall can only be remotely accessed by a limited number of users.

Network connectivity dramatically changes the risk profile for DIT system security. A network connected to the Internet is potentially vulnerable to unauthorized access, which makes server operations, applications and network devices exposed to the risk of being infected with malicious viruses and worms. According to the System Administration, Audit, Network, and Security Institute (SANS), to achieve overall security, a layered approach needs to be addressed and protected so overall security is achieved.

Some of the generally accepted practices that RPS is currently following are:

Generally Accepted Practices	DIT in compliance
All accounts use strong passwords and the default passwords have been changed	**Yes**
Packets with spoofed IP addresses are not allowed within the network	**Yes**
Unprotected file sharing and trust relationships are not allowed	**Yes**

As a result of the review of the network environment, the following conditions were noted:

RPS DIT lacks intrusion prevention and detection systems

- The audit identified that RPS DIT lacks intrusion prevention and detection systems. These systems are essential to enhance the perimeter security of the network by detecting external attacks and blocking penetration of the perimeter firewall. The Network Operations Group has submitted a budget request for the purchase of the IDS/IPS for the fiscal year 2009, however has not received approval.
- RPS has never conducted a network security intrusion detection analysis. This analysis involves an evaluation of the configuration of the external firewall, computer networks, and network configuration of internal infrastructure equipment. A network security intrusion detection analysis would be useful in verifying that the security controls in place at RPS DIT are working effectively. The Network Operations Group has submitted a budget request for a third party vendor to conduct a

network security intrusion detection analysis of RPS's network environment.

- The Network Group is not required to scan their external network on a routine basis. Routinely scanning the network will allow the group to notice any changes in firewall rules. Any changes should be traced back to firewall configuration changes.

Recommendations:

34. Purchase and install an intrusion detection system and intrusion prevention system for the external firewall.

35. Increase the amount of logging and monitoring for network security.

36. Hire a consultant to conduct a network security intrusion detection analysis to verify security controls in place at RPS DIT are working effectively.

37. Scan the RPS DIT network on a routine basis to create a baseline of open ports and review output for changes.

Wireless Technology Security Infrastructure

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network devices, for instance, allow users to move their laptops from place to place within offices and school rooms without the need for wires or losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs.

Auditors reviewed the wireless configurations of several access points for RPS. All of the wireless configurations contained the same controls and were configured in a uniform fashion. Some of the security features included within the wireless access point configurations were as follows:

RPS has a consistent wireless infrastructure configuration, which is desirable

- The default passwords have been changed on the wireless access points.
- RPS DIT is using network authentication (username and password) along with a static configured procedure for authentication that is different than factory settings.
- Access to the RPS network is separated by two functional virtual local area networks (VLAN) for the wireless environment. The wireless VLAN that is used by RPS DIT end-users is separated into the student and administrative side. Only the administrative side allows for a direct connection to the AS/400.
- Upon examination, wireless setting on computers at three schools appeared to be consistent and provided adequate security. The configuration of the wireless access appeared to be adequate.

It appears that RPS DIT has adequate basic controls over its wireless network services in the above areas.

However, the following conditions still exists:

Written policies and procedures are needed in this area

- The Network Operations Group does not have formally documented policies and procedures outlining how wireless access points should be configured. Although audit testing found no issues with the current configuration of the access

point, documented procedures are necessary for maintaining consistency in the future.

RPS DIT needs the capability to scan their network to detect unauthorized routers

- The Network Operations Group does not have tools available to scan their network for unauthorized wireless routers. They must check for unauthorized wireless routers on their network on a routine basis to ensure that students, faculty and staff are not installing their own personal equipment on the network. Without a tool that is designed to look for an unauthorized wireless router, finding an unauthorized router is difficult.

Recommendations:

38. Create formal policies and procedures to secure the wireless access points to ensure that all of the security settings are adhered to.

39. Create procedures and purchase network tools that will find unauthorized wireless routers on their network.

Active Directory

Active Directory is the integrated, distributed directory service that is included with Microsoft Windows to provide an authentication process for the network. With Active Directory, once a user logs into Windows with proper credentials, it will automatically unlock all applications or services utilizing Active Directory.

RPS DIT is in the preliminary stage of implementing Active Directory. There are no organization-wide policies that have been written or approved. RPS DIT personnel understand the importance of the implementation of Active Directory and have submitted an RFP for a third party vendor to assist with the policies and procedures for implementation. According to RPS DIT, they are in the process of having all of RPS servers authenticating through Active Directory. The

current security settings for RPS Active Directory were reviewed and deemed adequate.

Some of the generally accepted practices outlined for active directory authentication that RPS is following include:

Generally Accepted Practices	DIT in compliance
Authentication should be required for all accounts	**Yes**
Passwords should be at least 6-8 characters long and should provide adequate complexity (e.g., a mixture of upper and lower case letters, numeric, and special characters)	**Yes**
Passwords should automatically expire every 30-90 days	**Yes**
Multiple failed password attempts (e.g., 3-5 failed guesses) should automatically disable the ID for a specified period of time	**Yes**
All successful or unsuccessful attempts to use a password to log in should be logged	**Yes**

Recommendations:

40. Create organization-wide Windows Active Directory policies and procedures based on industry best practices.

41. Include revision and review dates in the updated policies and procedures.

42. Implement Active Directory across the network to strengthen the overall network security.

43. Create and implement a comprehensive and effective strategy for the rollout of Active Directory to help with network management and user administration.

44. Log and monitor Active Directory events for users on the network once the organization-wide rollout of Active Directory takes place.

Asset & Contract Management

The Asset and Contract Management section of the report will discuss the following:

- IT Data Center Physical Security
- Service Level Agreements
- Hardware Maintenance
- Software Licenses
- IT Fixed Assets Inventory
- Electronic Communication (Email)

IT Data Center Physical Security

Protection for computer equipment and personnel requires well-designed and well-managed IT Data Center physical site security facilities. The process of managing the IT Data Center physical site security environment includes:

- Defining the physical site security requirements;
- Selecting appropriate facilities; and
- Designing effective processes for monitoring environmental factors and managing physical site security access.

Effective management of the IT Data Center physical site security environment reduces business interruptions from damage to computer equipment and personnel.

Auditors verified through general observations that the RPS DIT Data Center has secured locks that require swipe cards, and visitors were accompanied by authorized RPS DIT staff when entering the data center. Auditors reviewed the process of a guest signing the visitor log and obtained a copy of the log for review. This manual process was

deemed adequate for assuring that only authorized personnel enter the data center.

In July 2007, RPS DIT relocated to their Richmond Training Center North location. In order to determine the cost effectiveness of the move, the Office of the City Auditor secured the services of PlanIT Technology Group, an expert consultant in the field of data center design and operations to:

1. Review the work and costs associated with the July 2007 relocation of the RPS IT Data Center to the new site;
2. Render an opinion as to the return on the City's investment in the RPS IT Data Center;
3. Review the new IT Data Center environment and assess what was delivered and where there might be opportunities to improve the delivered solution, if any; and
4. To provide documented findings and recommendations for areas for improvement.

RPS DIT needs to implement the consultant's recommendations

The consultant's recommendations were as follows:

1. Fire suppression
   - An FM 200 type system should be installed.
   - Room should be sealed off from core.
   - Budgetary Estimate: $18,000.
2. HVAC
   - Current systems should be stress tested and the installation of a humidification system should be considered. (Short term)
   - Current systems should be replaced with CRAC as soon as possible.
   - Budgetary Estimate: $25,000 (Two Liebert Challenger/3000).

- The outside heat pumps and the backup generator have been fenced in but access to these units would be easy. It is recommended that barbed wire be installed to harden this area.

Based on the current review, the above recommendations have not been implemented.

Recommendation:

45. Implement recommendations from PlanIT Technology Group Inc.

Service Level Agreements

A Service Level Agreement (SLA) is a contract that exists between a customer and its service provider. The agreement records the common understanding about services, priorities, and responsibilities.

To ensure that vendor and consultant services meet business requirements, clearly defined roles, responsibilities and expectations should be established. There must be a service level agreement established to document these requirements. In addition, appropriate performance measures need to be included.

DIT does not have a method to track and evaluate vendor services

Currently RPS DIT does not have a method to track and evaluate vendor services. Without proper evaluation of performance, RPS DIT cannot effectively and accurately determine vendor compliance of the system service level agreements and value received from the contract.

Copies of contracts with vendors were not available for audit review

During fiscal year 2007, RPS DIT provided supporting documentation outlining spending on service contracts totaling $424,249.38. However, they were only able to provide a copy of an actual service level agreement for review for one provider, which was for service on the AS/400 operating system. No further information or examples

could be provided for review concerning whether contracts are reviewed by a specific individual on a consistent basis.

Effective management of third-party services minimizes the business risk associated with non-performing suppliers

According to COBIT best practices, "effective management of third-party services minimizes the business risk associated with non-performing suppliers. Third-party services are optimized when contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the measurers."

Without structured policies and procedures for Service Level Agreements, there is a risk that contractual services are not:

- Identifying and categorizing supplier services;
- Identifying and mitigating supplier risk; and
- Monitoring and measuring supplier performance

Recommendations:

46. Create formal policies and procedures to properly monitor Service Level Agreements. The policies must address the monitoring of the service delivery and provide a mechanism to verify, measure and ensure adherence to written agreements.

47. Use performance measures to evaluate vendor and consultant services.

Hardware Maintenance

Hardware maintenance deals with the process of maintaining, servicing and performing preventive maintenance on computer equipment. Hardware maintenance agreements typically outline the expectations and scope of services provided. Audit review found that the maintenance process for RPS mission-critical equipment is adequate.

Software Licenses

A software license is a legal document that grants permission for the use of the software. The license also informs the user that the vendors have registered copyrights for the use of software. Copying or using the software without permission is illegal.

Severe penalties are applicable for infringement of copyrights

As a result of the recent increase in software piracy, the major software developers such as Microsoft, Adobe, and McAfee formed an organization called the Business Software Alliance (BSA) to educate and enforce software license compliance on behalf of its members. Copyright infringement is a criminal offense with penalties ranging up to a $500,000 fine or up to five years imprisonment for a first offense, and up to a $1,000,000 fine or up to 10 years imprisonment for subsequent offenses. BSA offers rewards of up to $1,000,000 to individuals who come forward and report software piracy by their current or former employers. This is a significant incentive for any individual to report copyright infringement if occurring at RPS DIT.

Potential exists for installation of unauthorized software on RPS computers

For a diverse organization such as Richmond Public Schools, where thousands of computers are being used, the potential exists for users to install unauthorized and unlicensed software on the computer assigned to them. RPS DIT does not have a definitive list of all of their software

licenses and accordingly, they are not in the position to verify the existence of licenses for all software copies in use at RPS DIT. This exposes RPS DIT to possible legal liabilities for copyright infringement and public embarrassment.

RPS DIT has neither performed a software license audit nor has a list of all software licenses

In identifying the weakness, RPS DIT has created an in-house asset management database to help keep track of the software licenses. The in-house software asset management system, Software Licensing Asset Manager (SLAM) allows for the tracking of software. This SLAM program was currently being populated during the time of the audit test work. RPS DIT has not completed inputting the software license listing into SLAM. Also, RPS DIT has not performed a software license audit. In addition, RPS DIT must consider implementing the LANDesk Asset Manager Module to enhance its ability to track and inventory computers and software applications.

It was not possible to determine whether RPS DIT holds proper licenses for software installed on all of its machines. Several reasons, as listed below, prohibited the auditors' ability to determine proper licensing of software.

1. The number of enterprise licenses that RPS DIT needs could not be determined.
2. RPS DIT does not have any other additional records of the total inventory for their computers, which prevented obtaining the accurate information needed to perform a comprehensive study.
3. RPS DIT also lacks information about all software installed on their computers. This situation not only prohibits RPS DIT's monitoring of software licensing compliance, but has a

significant impact on their ability to provide support to the users.

Recommendations:

48. Centralize RPS wide acquisition, installation, and upgrades of software. (RPS DIT is in the best position to accomplish the centralization of software management.)

49. Establish procedures to ensure employees are made aware of RPS DIT's software policy and require their acknowledgement in writing.

50. Prohibit users from installing and deleting any software on computers assigned to them. Allow only RPS DIT personnel the ability to install and delete software on computers. All software that does not pertain to school operations must be deleted.

51. Finish populating the centralized library for all software and licenses documentation into the SLAM (Software License Asset Management) system so that RPS DIT can readily and accurately determine the software licenses that they have purchased.

52. Once the SLAM database is fully populated and the LANDesk Asset Manager Module is being fully utilized, conduct a software license audit.

IT Fixed Assets Inventory

DIT conducted a physical inventory in February 2008. RPS' Fixed Asset System contained 32,138 pieces of IT equipment at the time of the inventory. The IT equipment in the fixed asset category includes all computers, laptops, computer related devices, printers, scanners, etc. The total number of physically inventoried IT equipment which matched the Fixed Asset System was 18,683 or only 58% of the equipment on the Fixed Asset System record. This means that RPS DIT personnel could not locate 13,455 or 42% of the items in the fixed asset system. This information is depicted in the following table:

IT equipment in the Fixed Asset System	32,138
Assets identified through physical inventory matching Fixed Assets	18,683
Unidentified Assets	**13,455**
Percentage unidentified	**42%**

Due to significant discrepancies in asset verification, errors may exist or assets may be missing

During the physical inventories, RPS DIT found 21,142 pieces of IT equipment in their physical inventory. This means that at least 2,459 (21,142-18,683) items inventoried were duplicate items or were not on the Fixed Assets System. It appears that there is a possibility of a significant number of errors in RPS' fixed assets system. However, the possibility of missing fixed assets cannot be ruled out.

RPS DIT does not have an adequate number of licenses for an application used for tracking and monitoring assets

RPS DIT purchased an application called LANDesk to track their hardware and software. LANDesk is an enterprise application that has a module that allows system managers to track and monitor the personal computers and the software installed on the computers that are on the network. However, the auditors found that RPS DIT did not purchase an adequate number of licenses for the LANDesk application. Audit inquiries revealed that RPS DIT possesses only 76% of the total licenses needed for this application. Due to the inadequacy of licenses, RPS DIT may not be able to identify all of the errors in records and missing assets.

Recommendations:

53. Resolve the hardware asset inventory issues from 2/27/2008 so that RPS DIT can create an accurate baseline of their computer assets.

54. Purchase an adequate number of LANDesk licenses to enable the Asset Management Module to be fully utilized on all desktops and laptops.

Electronic Communication (Email)

Email is an electronic means of communicating. In order for email to be effective in a work environment, the communication needs to be reliable and secure. Organizations need to have acceptable use policies outlining how email may be used. It is a common practice for organizations to require a signed affidavit from employees affirming they have read the policy before granting access to their email systems. The policy needs to be clear and concise in illustrating how users can and cannot use the organization's email system.

Guidelines for acceptable use of email are vague and incomplete

The RPS DIT procedures for using email are included with the acceptable Internet use policy for staff. The RPS DIT guidelines outlining acceptable email usage are vague and incomplete.

Contract with email provider was not available for audit review

The current email system used by RPS is a web based application that provides free email service to K-12 schools. Their email system is accessed through the RPS website for any RPS member who has access to the Internet. The only email equipment required for RPS to have on its network is an email relay to the provider. The external firewall rules for the email relay were reviewed. The email service is limited to inbound and outbound traffic to and from the static IP address of the provider. All other email traffic is adequately blocked for RPS email.

The service level agreement between the vendor and RPS for outsourcing the email service was requested several times from RPS DIT. Their personnel were not able to provide contract documentation between Richmond Public Schools and the provider.

RPS staff stated that they have been unable to access their email because of extended downtime issues on the system in several different

Staff reported that the free vendor services are unreliable

instances. According to RPS DIT, when the physical location of the provider's server and operations changed locations, downtime increased. During interviews, RPS DIT staff indicated that the email system has lost several emails or delayed delivery of emails during many extended downtimes. These deficiencies are outside of DIT's ability to fix and are the responsibility of the provider. The backup and recovery function of the email system lies completely with the service provider. RPS DIT's only course of action is to contact the vendor and report the problem. This appears to be a significant issue as the security and reliability of a communication system is left to a vendor against whom RPS DIT has limited recourse.

RPS has limited recourse against the provider for problem resolution

RPS DIT could not provide dates and the extent of the email system downtime or other performance metrics, as they do not monitor this information. In addition, RPS DIT does not receive performance metrics from the service provider. RPS DIT's only recourse for system issues is to contact the vendor and ask the vendor to correct the deficiencies. RPS DIT has no control over the resolution process.

The decision to use the low cost email services must be revisited

The auditors were informed that RPS DIT decided to change their existing email service to the free system in order to realize savings. The choice of other software would have required them to purchase other hardware, maintain and backup email servers. The rationale of this decision needs revisiting. A cost versus benefit analysis must be conducted to evaluate the prudence of this decision.

Recommendations:

55. Conduct a cost benefit analysis to determine if the performance of the current email system is effectively meeting RPS needs based

on the cost savings, opposed to using Microsoft Outlook or other standard email products.

56. Create email policies and procedures that outline the acceptable and unacceptable use of the system and communicate the policies to the RPS employees.

Staffing

A competent workforce is acquired and maintained for the creation and delivery of IT services. This process is critical, as employees are considered an important asset group. IT governance and the internal control environment are heavily dependent on the motivation and competence of personnel.

Staffing

As technology programs evolved in RPS, the need for technical expertise arose in several areas such as programming, networking, support, web development, and instruction. Over the years, RPS staffed positions to meet the Virginia Department of Education's recommended staffing ratios for technical support and instructional technology resource teachers. In response to recommendations made by the Office of the City Auditor's report issued in February 2007, RPS leadership has been reevaluating its IT staffing needs.

A consultant conducted an IT Staffing Study but did not evaluate if RPS DIT is optimally staffed

To assist RPS, the Center for Educational Leadership and Technology (CELT) conducted a study of the organizational structure of the technology department. Based on the auditor's review of the consultant's report, an evaluation of optimal staffing levels was not part of the study. This report presented a plan for reorganizing those jobs into an Information Technology and Communications Services (ITCS) department that is more service-oriented, customer-centric, and functionally-defined.

Status on RPS Implementing CELT Recommendations

The following is the summary of the auditors' evaluation of implementation of the consultant's recommendations:

Recommendation	Action Taken
Reorganize/merge units	Effective 07/01/08 RPS merged Telecommunication with the IT department to form the new group of Information Communications and Technology Services (ICTS).
Department staff should be clustered by functions	As part of the reorganization, various sections were clustered together based on job function.
Implement a project management approach	RPS created a Project Management Office (PMO) and hired relevant staff and management positions.
Revise job descriptions	RPS revised all job descriptions.
Hire adequately trained personnel	Personnel who do not possess the qualifications for the positions to which they are assigned are given one (1) year to acquire those qualifications (certifications).

The auditor verified that RPS DIT has implemented the above recommendations from the CELT study. As mentioned, the study did not address whether the IT organization is appropriately staffed and this was outside the purview of the audit.

Follow-up on Previous IT Audit Recommendations (*Richmond Public Schools Audit Report #2007-06*)

Auditors followed up on 15 IT recommendations made in the May 2007 audit

In June 2007, the City Auditor's Office released an audit of Richmond Public Schools in which 15 IT related recommendations were issued. RPS has implemented three recommendations and still do not concur with four. RPS has eight recommendations outstanding as depicted in the table below:

Original Recommendations	Status
1. *Lease computers rather than purchasing them in order to smooth budget spikes, facilitate standardized personal computers, and provide an effective disposal strategy for used machines.*	For any new project or software upgrade requiring a newer server, RPS is now leasing the servers. RPS indicated that a consultant will be hired to create and manage their PC replacement initiative utilizing the leasing option. Also, RPS management indicated that they were pending further discussion with the City of Richmond DIT to use their leasing program in 2009.
2. *Consider negotiating inclusion of technical support including replacement parts, loaner programs, and expected service levels when entering into leasing agreement.*	As stated in the recommendation above, RPS indicated that a consultant will be hired to create and manage their PC replacement initiative utilizing the leasing option. Also, RPS management indicated that they were pending further discussion with the City of Richmond DIT to use their leasing program in 2009.
3. *RPS's Department of Information Technology should assist in the planning and implementation of all new systems.*	RPS now schedules weekly project meetings with the project sponsors, where DIT assists in the initiation, planning, execution, controlling and closing of projects in accordance with the Project Management Institute standards.
4. *Implement thin client technology in the classroom to better serve teacher and student users while reducing administrative costs.*	RPS is in the analysis phase to determine which areas to convert to Thin Client. The analysis phase is scheduled for completion by the end 2008. This recommendation was not scheduled to be reviewed during the recent follow-up review period.
5. *Establish a policy that requires a representative from user*	RPS is in the process of establishing a Project Management Office (PMO)

groups be involved in the selection and implementation of the software applications.	aligned with the balance scorecard. This will enable RPS to have representation in all selection and implementation of software. This recommendation was not scheduled to be reviewed during the recent follow-up review period.
6. *Take advantage of the Web-X Training Session offered by FAMIS and become a member of ListServ to assist in staff training.* 7. *Obtain additional training from FAMIS, if needed, to gain a full understanding of the features and capabilities.*	The implementation of these two recommendations is still in progress and were not scheduled to be reviewed during the recent follow-up review period.
8. *Contact FAMIS to explore the possibilities of interfacing the application with CIMS. (By interfacing the systems, the need for double keying and recordkeeping would be eliminated. The systems should be able to share data such as chart of accounts, employee profiles, vendor profiles, fixed assets and accounts payable data)*	The implementation of this recommendation is still in progress and it was not scheduled to be reviewed during the recent follow-up review period.

The auditor was informed that the eight open recommendations listed above are in the process of being implemented.

The recommendations for implementing Voice over Internet Protocol (VoIP) technology were originally not concurred with by RPS DIT. Based on pricing offered to the City of Richmond by Verizon, the City Auditor's office had estimated a significant annual saving of $453,400 due to implementation of this technology.

During this review, the auditor was told that they have implemented the technology at the Richmond Training Center with plans to go forward with implementation at other locations.

Recommendation:

57. RPS DIT must develop a formal documented plan to implement VoIP technology for other school district locations.

Attachments

Attachment A – RPS Management Responses

Attachment B – PlanIT Data Center Report

Attachment C – CELT RPS IT Report

THIS PAGE LEFT BLANK

INTENTIONALLY

MANAGEMENT RESPONSE & FOLLOW-UP FORM
RPS INFORMATION TECHNOLOGY - REPORT #2009-05 - FEBRUARY 2009

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
1	**Conduct an organization-wide IT risk assessment and compile a formal mitigation plan.**	Y	RPS has contracted CELT Corp. to assist Information Communication Technology Services (ICTS) in developing a new comprehensive district-wide technology plan that includes an assessment and mitigation plan.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Director of ICTS		Apr-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
2	**Periodically, evaluate the relevance and adequacy of the risk assessment and the mitigation plan.**	Y	Once the technology plan is complete, RPS will periodically evaluate relevance and risk assessment on a quarterly basis.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Director of ICTS		Jul-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
3	**Create disaster recovery and business continuity plans in accordance with generally accepted practices such as the COBIT framework, to reduce the impact of a major disruption on key business functions and processes.**	Y	RPS is reviewing and revising our existing Disaster Recovery and Business Continuity Plans in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Director of ICTS		Dec-10
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
4	**Test the Disaster Recovery and Business Continuity plans on a regular basis.**	Y	Upon completion of the revised Disaster Recovery and Business Continuity plans, RPS will test the plan three (3) times a year.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		Dec-10
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
5	**Provide all staff with regular continuity planning training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Modify the training as necessary based on the test results.**	Y	All central level and school level administrators will receive disaster recovery training. The ICTS director will provide quarterly status report to the Superintendent's cabinet
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		On Going
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
6	**Develop a disaster recovery solution to provide an appropriate computer facility to resume RPS' business during and after disasters.**	N	RPS has located a "Warm Site" locally for computer operation redundancy. This will allow RPS to resume 75% of operations within one (1) hour in case of a disaster

	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager		Closed
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
7	**Create an effective process for monitoring the vendor providing the disaster recovery facility by clearly defining the roles, responsibilities, expectations, service levels and performance indicators.**	Y	RPS will establish an effective monitoring process that will define the roles, responsibilities, expectations, and performance indicators.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager		Apr-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
8	**In accordance to industry best practices, create appropriate policies, standards and procedures that clearly outline the change management process.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Process and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Change Management Process.**
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		On Going
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
9	**Create a Change Advisory Board or similar mechanism and describe pertinent roles and responsibilities for personnel involved.**	Y	The Project Management Oversight Committee's (PMOC) serves as Change Advisory Board.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		Closed
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
10	**Require the Change Advisory Board or similar group to review and approve all change requests and related metrics based on established change management policies, standards, processes and procedures.**	Y	The Project Management Oversight Committee (PMOC) reviews and approves all change requests.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		Closed
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
11	**Educate users and IT professional about processes and procedures related to requesting and implementing system changes.**	Y	All requests for system changes are recorded via the Service Desk with a Ticket Number. Users were trained in this process in August 2008.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	DSS & Data Manager		On Going

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
12	**Establish a formal configuration management policy in accordance with best practices such as COBIT and implement proper procedures and supporting tools to comply with the policy.**	Y	As noted in the audit, ICTS is in compliance with best practices of system configuration management. However, ICTS is currently working on implementation using "Soft Landing" which is a
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager and DSS & Data Manager		Jul-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
13	**Update policies and procedures addressing overall IT control environment security concerns.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Use Guidelines and Common Forms of Computer Abuse.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Director of ICTS		Mar-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
14	**Create network security policies and procedures based on a risk analysis, best practices, and management's revised mission and vision. The new policies and procedures must include version control, training and a communication plan.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS P***rocesses and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Network Standards and Network Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Telecommunications & Network Manager		Mar-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
15	**Implement a security awareness program to inform users of RPS DIT security expectations. A signed security form must be created and retained by RPS DIT to ensure staff is held accountable for security awareness.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Security Technology Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Human Resources Director and Director of ICTS		Jul-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
16	**Create an annual training plan to ensure that security standards are reinforced.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Security Technology Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		Jul-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
17	**Create incident response policies and processes to ensure that all incident responses are handled efficiently and effectively.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Policy Violation Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Telecommunications & Network Manager		Jul-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
18	**Create AS/400 systems operations and applications policies and procedures based on industry best practices. To ensure adherence to the new policies, a communication and training plan must be implemented.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **iSeries (formally AS/400) Standard Operation Procedure.** The communication plan and training will be provided to staff.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager and DSS & Data Manager		Aug-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
19	**Establish operational standards and security guidelines for securing, creating and updating web applications.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Web Application Procedures.**

	RESPONSIBLE PERSON/TITLE		TARGET DATE
	DSS & Data Manager		Aug-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
20	**Create policies and procedures for the DB2 databases security and operational settings of the AS/400.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Security Standards for Application Administration.**
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager		Dec-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
21	**Create a formal set of policies to address data management. Include the development and execution of architectures, standards, practices and procedures that outline the full data lifecycle in accordance with best practices and management's new vision. The updated data management policies and procedures must include revision and review dates.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Server(s) Backup Procedure and Data Protection-Authorization Control Standards.**
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager and DSS & Data Manager		Aug-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
22	**Implement a communication and training plan to ensure adherence to the new policies.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. A communication and training plan is included in the project plan. As each process and procedure is approved by the PMOC, ICTS will communicate and provide training for all stakeholders."
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager and DSS & Data Manager		Aug-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
23	**Create a formal process of recording all successful and unsuccessful backups to document the validly and the reliability of the backup process.**	Y	The outcome of the Processes and Procedures (**2P's Project - <u>Project ID 010</u>**) project will be the ICTS Processes and Procedures Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Server(s) Backup Procedure and Data Protection-Authorization Control Standards.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Aug-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
24	**Create detailed policies and procedures for the Service Desk outlining the processes and expectations of Service Desk personnel.**	N	The audit of Information Communication Technology Services (ICTS) is for the twelve months ended December 31, 2007. The Service Desk was created in June 2008 and has a procedures manual which outlines the processes and expectations of the Service Desk personnel.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Closed

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
25	**Identify, create, and monitor meaningful metrics to develop baseline standards and expectations of the Service Desk.**	Y	The audit of Information Communication Technology Services (ICTS) is for the twelve months ended December 31, 2007. The Service Desk was created in 2008 and has a procedures manual which outlines the processes and expectations of Service Desk.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Closed

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
26	**Implement a comprehensive and effective System Development Life Cycle methodology that clearly defines the roles and expectations of the IT staff responsible for implementing, changing, testing and maintaining systems and applications.**	Y	The outcome of the Processes and Procedures (**2P's Project - <u>Project ID 010</u>**) project will be the ICTS ***<u>Processes and Procedures</u>*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Change Management Process.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager and DSS & Data Manager		Dec-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
27	**Establish a system security baseline for the AS/400. Require the system control values of the AS/400 to comply with industry (IBM and ISACA) benchmark settings.**	Y	RPS is in compliance with benchmark settings established by IBM and Comprehensive Management Systems. Essential application software supersedes the recommended settings. This application provides these features for the items cited.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Jul-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
28	**If essential application software requirements prevent benchmark settings from being used, establish compensating controls.**	Y	RPS is in compliance based on the setting requirements for our business application, Comprehensive Information Management System (CIMS).
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Dec-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
29	**Assess the feasibility of turning on the audit trail feature to provide the ability to review audit logs ensuring proper system tracking and accountability.**	N	The audit trail logging feature is part of the original operating system. Using the logging feature would exceed existing storage capacity. However, RPS has other audit features such as a "performa" and history files.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech Services Manager		Jul-08
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
30	**Require managers to have a signed access change form for all system access changes. The manager's signature should be verified against an authorized signature list for granting, changing and terminating access.**	Y	The outcome of the Processes and Procedures **(2P's Project - <u>Project ID 010)</u>** project will be the ICTS ***<u>Processes and Procedures Guidelines</u>*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Access, Security and Control of Data and Information Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager and DSS & Data Manager		Mar-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
31	**Discontinue email as a method of requesting changes in access privileges. Discontinue the use of faxed requests until an authorized signature list is put in effect. Use an alternative appropriate mechanism to request and approve changes in access privileges. Evaluate cost benefits of implementing an automated workflow solution.**	Y	RPS will perform the analysis and determine the best economic solution.

	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		Dec-10
#REF!			
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
32	**Implement system application controls that will maintain an accurate and reliable audit trail for previous and current vendor checks. If system controls cannot be applied, implement compensating controls to provide the historical audit trail to track previous vendor payments.**	Y	RPS will perform the analysis for this and we determine the best economic solution.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	DSS & Data Manager		Aug-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
33	**Require Programmers to make all changes in the test environment. Require a different staff member to test all changes prior to making the approved changes to the production environment.**	Y	RPS currently makes all changes in the test environment and requires a different staff member to test all changes prior to making changes to the production environment.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager and DSS & Data Manager		Jul-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
34	**Purchase and install an intrusion detection system and intrusion prevention system for the external firewall.**	Y	RPS agrees with recommendation and we are currently reviewing quotes for this software.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Telecommunications & Network Manager		Jan-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
35	**Increase the amount of logging and monitoring for network security.**	Y	RPS agrees with recommendation (Project ID 030) and is in the process of increasing server capacity to accomplish this task.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager and Telecommunications & Network Manager		Mar-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
36	**Hire a consultant to conduct a network security intrusion detection analysis to verify security controls in place at RPS DIT are working effectively.**	Y	RPS has hired a consultant and we are presently testing any malicious access to our network.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Telecommunications & Network Manager		Closed
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
37	**Scan the RPS network on a routine basis to create a baseline of open ports and review output for changes.**	Y	RPS currently conducts routine network reviews and will create a formal document for this process.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Telecommunications & Network Manager		Jan-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
38	**Create formal policies and procedures to secure the wireless access points to ensure that all of the security settings are adhered to.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Wireless Standards**.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Telecommunications & Network Manager		Mar-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
39	**Create procedures and purchase network tools that will find unauthorized wireless routers on their network.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Wireless Standards.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Telecommunications & Network Manager		Apr-09
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
40	**Create organization-wide Windows Active Directory policies and procedures based on industry best practices.**	Y	Active Directory implementation , Project #107, has been established, however, because of budgetary constraints RPS is unable to expand district-wide.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		On Hold
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
41	**Include revision and review dates in the updated policies and procedures.**	Y	RPS has purchased, implemented and received training in "The Policy Management Tool" in order to manage the ***Processes and Procedures Guidelines.***
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		On Going
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
42	**Implement Active Directory across the network to strengthen the overall network security.**	Y	Active Directory implementation , Project #107, has been established, however, because of budgetary constraints RPS is unable to expand district-wide.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		On Hold

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
43	**Create and implement a comprehensive and effective strategy for the rollout of Active Directory to help with network management and user administration.**	N	Active Directory implementation , Project #107, has been established, however, because of budgetary constraints RPS is unable to expand district-wide.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
44	**Log and monitor Active Directory events for users on the network once the organization-wide rollout of Active Directory takes place.**	Y	Active Directory implementation , Project #107, has been established, however, because of budgetary constraints RPS is unable to expand district-wide.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		On Hold

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
45	**Implement recommendations from PlanIT Technology Group Inc.**	Y	RPS will consider the PlanIT Technology Group recommendations in the upcoming FY2010 budget.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Director of ICTS and Tech & Services Manager		TBD

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
46	**Create formal policies and procedures to properly monitor Service Level Agreements. The policies must address the monitoring of the service delivery and provide a mechanism to verify, measure and ensure adherence to written agreements.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Vendor Management Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Department of Purchasing and Director of ICTS		Dec-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
47	**Use performance measures to evaluate vendor and consultant services.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Vendor Management Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Department of Purchasing and Director of ICTS		Dec-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
48	**Centralize RPS wide acquisition, installation, and upgrades of software. (RPS DIT is in the best position to accomplish the centralization of software management.)**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Software Acquisition and Management Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		Aug-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
49	**Establish procedures to ensure employees are made aware of RPS DIT's software policy and require their acknowledgement in writing.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010)** project will be the ICTS ***Processes and Procedures*** Guidelines in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Software Acquisition and Management Procedure.**
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		Aug-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
50	**Prohibit users from installing and deleting any software on computers assigned to them. Allow only RPS IT personnel the ability to install and delete software on computers. All software that does not pertain to school operations must be deleted.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Software Acquisition and Management Procedure**.
	RESPONSIBLE PERSON/TITLE		**TARGET DATE**
	Tech & Services Manager		Aug-09

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
51	**Finish populating the centralized library for all software and licenses documentation into the SLAM (Software License Asset Management) system so that RPS can readily and accurately determine the software licenses that they have purchased.**	Y	The outcome of the Processes and Procedures (**2P's Project - Project ID 010**) project will be the ICTS ***Processes and Procedures Guidelines*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Software Acquisition and Management Procedure.**

	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager and Department of Purchasing and DSS & Data Manager		On going
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
52	**Once the SLAM database is fully populated and the LANDesk Asset Manager Module is being fully utilized, conduct a software license audit.**	Y	The outcome of the Processes and Procedures (**2P's Project - <u>Project ID 010</u>**) project will be the ICTS ***<u>Processes and Procedures Guidelines</u>*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Software Acquisition and Management Procedure.**
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech & Services Manager		Aug-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
53	**Resolve the hardware asset inventory issues from 2/27/2008 so that RPS can create an accurate baseline of their computer assets.**	Y	This inventory was performed by RPS ICTS and presented to the board in February 2008. This discrepancy is the direct result of tracking surplus and transfers of donated equipment, calculators, film strip projectors, Word Processors and other computer related assets with only paper form of accountability dating back to 1967. In eliminating the error rate associated with written physical inventory, as of November 2008 we are currently implementing a direct electronic integration into CIMS. Every method possible will be used to reconcile the fixed asset system for these items.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech. & Services Manager		Dec-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
54	**Purchase an adequate number of LANDesk licenses to enable the Asset Management Module to be fully utilized on all desktops and laptops.**	Y	RPS has purchased the adequate LANDesk licenses and has assigned staff to track hardware and software. The computer disposal and redistribution process is currently in place to identify and reclaim used licenses. The redistribution process is currently being practiced.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Tech. & Services Manager		Oct-08
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
55	**Conduct a cost benefit analysis to determine if the performance of the ePals email system is effectively meeting RPS needs based on the cost savings, opposed to using Microsoft Outlook or other standard email products.**	Y	RPS has performed the cost benefit analysis.

	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		Dec-08
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
	Budget Constraints		
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
56	**Create email policies and procedure that outline the acceptable and unacceptable use of the system and communicate the policies to the RPS employees.**	Y	The outcome of the Processes and Procedures (**2P's Project - <u>Project ID 010</u>**) project will be the ICTS ***<u>Processes and Procedures Guidelines</u>*** in accordance to Information Technology Infrastructure Library (ITIL®) and best practices, required for operating as a 21st century department. Within these guidelines, there will be a section on **Email acceptable Use and Email Communication Procedure.**
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Director of ICTS		Apr-09
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
57	**RPS DIT must develop a formal documented plan to implement VoIP technology for other school district locations.**	Y	RPS is currently in the process of upgrading our network infrastructure that will give us the capability to implement VoIP depending on budget constraints.
	RESPONSIBLE PERSON/TITLE		TARGET DATE
	Telecommunications & Network Manager		Dec-10

THIS PAGE LEFT BLANK

INTENTIONALLY

Attachment A

Richmond Public School's DATA CENTER Relocation Costing Review

For

Office of the City Auditor, City of Richmond

April 8, 2008

RPS DATA CENTER Relocation Costing Review

Table of Contents

Scope

Decisions within the City of Richmond executive staff and the City of Richmond Public Schools (RPS) concluded that a move of the RPS Data Center from their downtown site to a new site at the Richmond Technical Center (RTC) would be needed.

The Office of the City Auditor was asked to review the work and costs associated with them move to the new site and to render an opinion as to the return on the City's investment in the RPS Data Center.

The Office of the City Auditor, City of Richmond has asked PLANIT to review the new environment and assess what was delivered and where there might be opportunities to improve the delivered solution, if any.

This analysis renders only an opinion and assessment of the environment to the extent of the information provided.

This assessment was created after interviews with City of Richmond Auditors, documentation provided by the Office of the City Auditor (see Appendix A), and an onsite visit on March 27, 2008.

Site Review Findings – Corrective actions

Physical (Data Center)

1. **Security**
    a. Data Center (DC) access is controlled by the use of electronic cards which are issued and monitored by the security manager.

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed was reasonable**.

        2. **Corrective Action:**
            a. **None**

2. **Space**
    a. The new DC has adequate square footage to support current and future growth.
    b. The floor is tile over concrete
    c. Ceiling is plenum with recessed florescent lighting. Duck work supporting the HVAC is installed in the open space providing for the air returns and air output.
    d. It was noted that cardboard boxes were stored in the DC (next to the UPS). As general practice paper/cardboard should not be stored in the Data Center.
    e. Data Center is clean, dry and well lit.

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed was reasonable.**

        2. **Corrective Action**
            a. **None, except as noted in point d. above.**

3. **Power**

    a. The new DC is protected by a Power Ware UPS which has a backup generator. The generator is tested monthly under full load. Fuel levels and fuel quality is tested during these tests.
    b. The UPS is monitored using Simple Network Monitoring Protocol (SNMP).

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed was reasonable**.

        2. **Corrective Action**
            a. **None**

4. **Data Racks**
    a. The DC uses new Wright Line Data Cabinets. These are state of the art with built in fans and PDUs. These cabinets are on average 50% utilized. There is a hot/cool layout allowing for correct air flow.
    b. Four post data racks are used to support Communication equipment and patch panels. These are correctly bolted to the floor.

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed was reasonable**.

        2. **Corrective Action**
            a. **None**

5. **Sensors**
    a. The DC has both smoke and temperature SNMP sensors.
    b. Site uses Closed Circuit Television (CCTV) outside the DC and generally throughout the building.

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed was reasonable**.

        2. **Corrective Action**
            a. **None**

6. **Fire suppression**
    a. The DC does not have a water sprinkler system installed.
    b. The DC does not have a FM200 type suppression system.
    c. The DC is not sealed from the core building. The out side walls have not been built using a fire grade sheetrock and these walls to not connect to the concrete ceiling.
    d. The only fire suppression available is two portable "dry" extinguishers – one outside the data center and one just inside the door.
    e. The data center has been built with glass windows allowing for the offices outside the DC to view the interior. This was done to allow for quick response to a fire. The assumption is that personnel will always be present and looking into the DC.

        1. **Cost Reasonableness:**
            a. **Based on provided documentation costing for work performed is questionable. As noted, the current environment does not follow current IT best practices of providing proper fire protection. For the existing system to work, personnel must not only observe a fire but also engage the fire to put it out with just two extinguishers.**

        2. **Corrective Action**
            a. **A FM 200 type system should be installed.**
            b. **Room should be sealed off from core.**
            c. **Budgetary Estimate: $18,000.00**

7. HVAC

a. The DC is cooled using two Carrier Infinity Series Heat Pumps. The concern is that these are not commercial grade and do not provide any humidification function. The DC was at 72 degrees at the time of the survey. The question was asked if a Stress Test had been conducted using only one unit. The answer was no.

b. Heat removal in a mission critical environment, like a data center, is one of the most essential yet least understood of all environmental IT processes. As technological advances are made – equipment shrinks – yet uses the same or more electricity than the equipment it replaced, resulting in more heat generation in these critical environments. The nature of a data center makes unique demands on an environmental control system and requires data center air conditioners (CRAC).

c. "Office" air conditioning systems are not designed to provide the precision or the reliability necessary to maintain the stringent requirements of a data center. Many elements must be considered when purchasing and installing CRAC; power requirements (today and future), air flow, humidification, filtration, size, and location.

1. **Cost Reasonableness:**
    a. **Based on provided documentation costing for work performed is questionable. A more compatible Computer Room Air Conditioner (CRAC) should have been architected and installed resulting in a less costly solution in line with data center best practices.**

2. **Corrective Action**
    a. **Current systems should be stress tested and the installation of a humidification system should be considered. (Short term)**
    b. **Current systems should be replaced with CRAC as soon as possible.**
    c. **Budgetary Estimate: $25,000.00 (Two Liebert Challenger/3000)**
    d. **The outside Heat Pumps and the Back up generator have been fenced in but access to these units would be easy. It is recommended that barbed wire be installed to harden this area.**

8. **Cable Management**
    a. Cable trays have been installed with both power and UTP/Fiber sharing. This meets code and is very efficient. There is ample room for additional Communication and Power cabling.

1. **Cost Reasonableness:**

    a. **Based on provided documentation costing for work performed was reasonable**.

2. **Corrective Action:**
    a. **None**

Summary assessment:

Apart from the issues noted, especially regarding Fire Suppression and HVAC, the Data Center provides for both current and future IT requirements extending out for at least three years based on conversations and documentation regarding growth expectations.

Physical (Communication Closet) – 2nd floor

1. **Security**
    a. Room access is by key and we had to ask the janitor for key.
        i. This room should have electronic card access installed.

2. **Rack**
    a. Room has a four post rack/bolted to floor.
    b. Rack is full and any additional IT equipment would require a second rack.
    c. There is room for one more rack

3. **Power**
    a. There is a UPS in the Rack which is connected to house power. This power cord is extended from the rack to the wall at about 4 feet off the floor. It would be easy to knock this out of the outlet.
    b. A new 120V quad isolated ground outlet should be installed closer to the rack.

4. **There is some non IT and general clutter – general cleaning would correct.**

Intermediate Distribution Frame (IDF) – 2nd floor

1. Rack
    a. There is one wall mounted rack (non swing).
    b. Cables are well managed.
    c. The fiber and switching equipment are powered using a APC surge protector – no UPS

Summary of review:

It was not within this SOW to consider if the building of a new Data Center was the correct course of action.

It is assumed that the costing to relocate the Voice Systems is correct and justified because a new build was required.

The RPS relocation project was comprised of multiple umbrella offerings.

There are multiple areas for improving the data center's capabilities, e.g., HVAC, fire suppression. In at least one case, HVAC, less money could have been spent for a better solution. In most other areas the space, the technologies and the equipment upgrades, e.g., cabinets, VoIP phones, have the capacity to scale to accommodate the forecasted growth and expansion of RPS.

This report does not render an opinion on whether tighter management of the procurement process or a selection of different vendors or technologies would have yielded a betters solution or less expensive solution.

THIS PAGE LEFT BLANK

INTENTIONALLY

Comment [IN1]:

Department of Information and Technology
Organizational Structure Review

July 26, 2008

Working Document- Internal Use Only

Prepared by

Center for Educational Leadership and Technology
199 Forest Street
Marlborough, MA 01752
Tel. (508) 624-4474
www.celtcorp.com

Table of Contents

1. Introduction

As technology programs have evolved in Richmond Public Schools (RPS), a need for technical expertise has arisen in several areas – programming, networking, support, Web development, and instruction. Over the years, the district staffed positions to address these needs, hiring a combination of permanent and contracted staff, and supplemented these to meet the Virginia Department of Education's recommended staffing ratios for technical support and instructional technology resource teachers. At the present time, and in response to recommendations made by the Office of the Richmond City Auditor in an official report issued in February 2007, describing their audit of Richmond Public Schools, district leadership has been reviewing the staffing of Department of Information Technology to determine whether it is at an effective level and to identify areas for improvement.

To assist the district, the Center for Educational Leadership and Technology (CELT) has conducted a study of the organizational structure of the technology department(s) at RPS. This report presents a plan for reorganizing those jobs into an Information Communication and Technology Services (ICCS) department that is more service-oriented, customer-centric, and functionally-defined.

2. Technology Organizational Structure

The organizational structure of the Department of Information Technology (DIT) has evolved over more than twenty years to address the district's technology-related needs and is shown in Figure 1. DIT consists of a manager, an office assistant, and seven groups: Records Management, Data Center Operations, Computer Service Center, Data Systems and Reporting, Technology Services, Technology Asset Administration, and Network Operations. While the charter of some of these groups is self-evident, a few have responsibilities that seem outside of their jurisdiction and areas of expertise. The responsibilities of each group are:

- Records Management – responsible for scanning and archiving student records and human resources information, and for managing transcripts. (4.5 FTE)
- Data Center Operations – responsible for configuring, maintaining, and supporting the district's 100 servers. In addition, this group is currently working on a virtualization project and positioning the district to move to Active Directory for real-time information access from multiple applications. (4 FTE)
- Computer Service Center – responsible for desktop support and maintenance throughout the schools and administrative centers. (13 FTE)
- Data Systems and Reporting – responsible for applications programming and support, as well as data reporting. In addition, this group is responsible for the district website, portal, and intranet as well as applications training. (12.5 FTE plus 2 interns)

- Technology Services – serves as the liaison between DIT and Instructional Technology (part of Curriculum and Accountability) (2 FTE)
- Technology Asset Administration – oversees the LANDesk implementation, tracking operating system and application software versions and updates (1 FTE)
- Network Operations – responsible for configuration, monitoring and support of all local area networks and network operations in all schools, including both hardwired and wireless. (2 FTE).

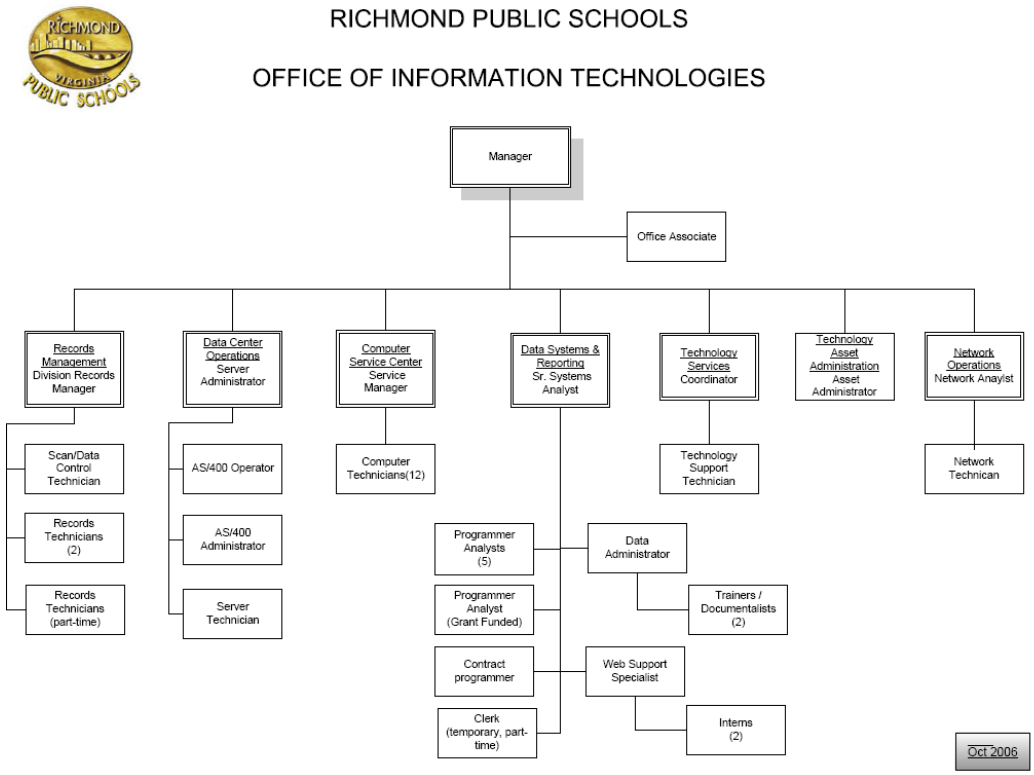


Figure 1. Department of Information Technology (DIT) Organizational Chart

The number of FTE listed for each group in the bullets above represent the number of FTE who are allocated to each group. Fully staffed, DIT consists of 39 FTE, including the manager, plus two interns. In addition, the Computer Services group has 5 contractors to meet the VDOE ratio for technical support. To assist with technical support and maintenance, including software installation and configuration at the desktop level, DIT has recently recruited a Student Technology Leadership team who will be trained and deployed over the summer.

2.1 Office of Telecommunications

In addition to DIT, the Office of Telecommunications is responsible for all Internet and telephony services within the district. The organizational structure of the Office of Telecommunications is shown in Figure 2. The Office of Telecommunications consists of a manager, an account technician, and an electronic systems maintenance group. The responsibilities of the individuals in these groups are listed below.

- Account Technician – responsible for collecting and updating E-Rate information and assisting with filings
- Electronic Systems Maintenance Group – responsible for the installation, configuration, repair, and maintenance of the district's telephone systems. In addition, this group is responsible for repairing electronic devices, such as telephones, switches, projectors, and VCRs. In addition, this group assists with maintenance and support of the security cameras.
- Manager of Office of Telecommunications – oversees departmental operations and is responsible for E-Rate filings, as well as telecommunications design.

Fully staffed, this office consists of 7 FTE.

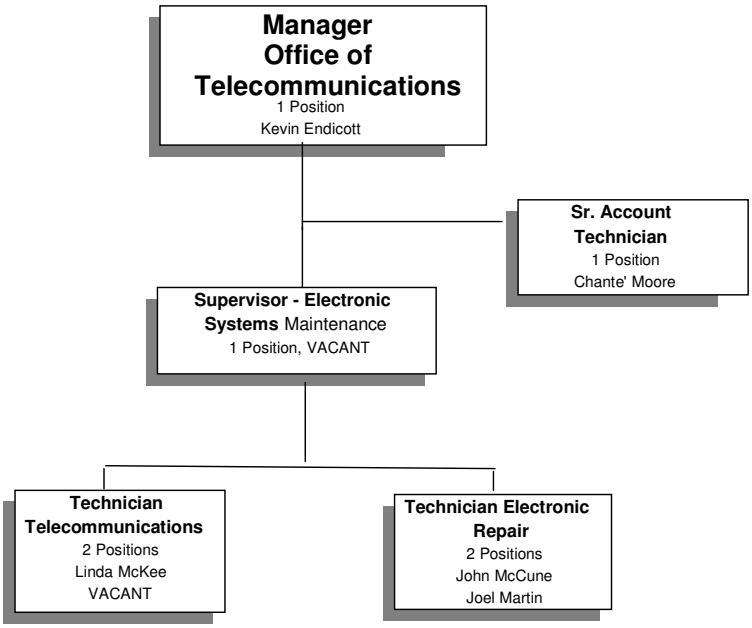


Figure 2. Office of Telecommunications Organizational Chart

2.2 Instructional Technology

Instructional Technology support is provided by the Instructional Technology Resource Teachers (ITRT). These individuals are assigned to schools and selected by the principals according to the VDOE ratio and report to the Instructional Technology Coordinator within the Curriculum and Accountability Division. The Instructional Technology Coordinator is responsible for the selection of instructional software and academic achievement software that is used in the schools. As previously stated, the Technology Services Coordinator serves as a liaison between the ITRTs and the DIT.

3. Review of Current Status

3.1 Silos

The current organization has resulted in a structure of "silos" or groupings of technical staff that address the tasks that are assigned to their groups but is not conducive to cooperation and collaboration. Because the culture of the department over the last several years has lacked intradepartmental communications, the groups within the department are not in the habit of working together to develop and implement a plan for a technology project. Each group has taken responsibility for their segment of a project, but until recently, there was not an overall project management approach. The individual who was hired as the project manager for technology refresh has been assigned to another position, supervising people rather than managing projects.

Under the current reporting structure, the DIT manager has 9 direct reports. Of the 7 groups within the department, 5 have 5 members or fewer. The Telecommunications manager has 2 direct reports. The supervisor under him oversees the remaining 4 members of the group.

3.2 Redundancy

Given the increasing use of Web-based applications, there is an increasing level of interdependency between DIT, Telecommunications, and Instructional Technology. Many applications are Web-based rather than server-based, and the WAN and LAN are critical to all district functions, including instruction, administration, and support services. The issues addressed by the Network Operations staff and by the Telecommunications staff are similar and require many of the same skills. While this does not imply that one can be simply substituted for the other, they should have a close working relationship and collaborate on network services.

As an adjunct to this, many of the operational support tools are available over the Web, including Remedy for reporting and tracking help requests; LANDesk for operating system and software management, and network management tools. Using these and other strategies, as well as providing additional training at the

school level, RPS can reduce the need for onsite technical support staff and centralize many of these services at the district level.

3.3 Job Descriptions

In general, job descriptions are outdated and do not reflect either the responsibilities of the position or the experience and proficiencies that are required to perform these activities. In some cases, individuals are in positions for which they do not have the qualifications or training. Recommendations for updating these job descriptions are included as an appendix to this study.

4. Recommendations

To address the technology-related needs of the Richmond Public Schools, CELT recommends reorganizing/merging the Department of Information Technology and the Office of Telecommunications. The new department, to be known as Information Communication and Technology Services (ICTS), will be functionally-organized, service-oriented, and aligned to RPS' strategic goals. Department staff will be clustered by function, to facilitate cross-training and better address the evolving needs of the district. By implementing a project management approach and developing processes based on the Information Technology Infrastructure Library, the department will improve their relationships with schools and administration and be more successful overall.

Staffing Alignment Process – To ensure that people are aligned to positions and job descriptions for which they have the training and experience, it is recommended that the revised job descriptions be adopted and that staff be assigned to the positions on the revised organizational chart for which they are best-suited. This is the equivalent of starting with a blank staffing chart and assigning people to the positions they fit. In most cases, people will be assigned to the same position as they currently hold, but with a slightly different reporting structure, such as the programmer analysts. In a few cases, where a position is being eliminated or redefined, or where someone has been filling a position for which he or she is not qualified, realignment and/or additional training may be necessary.

It is further recommended that personnel who do not possess the qualifications for the positions to which they are assigned will be given up to 1 year to acquire those qualifications (certifications, registrations, etc.). If not qualified at the time mandated, the employee may be non-renewed or may be reassigned to a position for which he/she is qualified, at the salary level commensurate with the new position

5. Revised Organizational Chart

The recommended organizational chart is depicted in Figure 3. The revised organizational structure is comprised of 5 major groupings which will accommodate the new directions of RPS and a project management office that will ensure that project implementations stay on track and aligned to district goals.

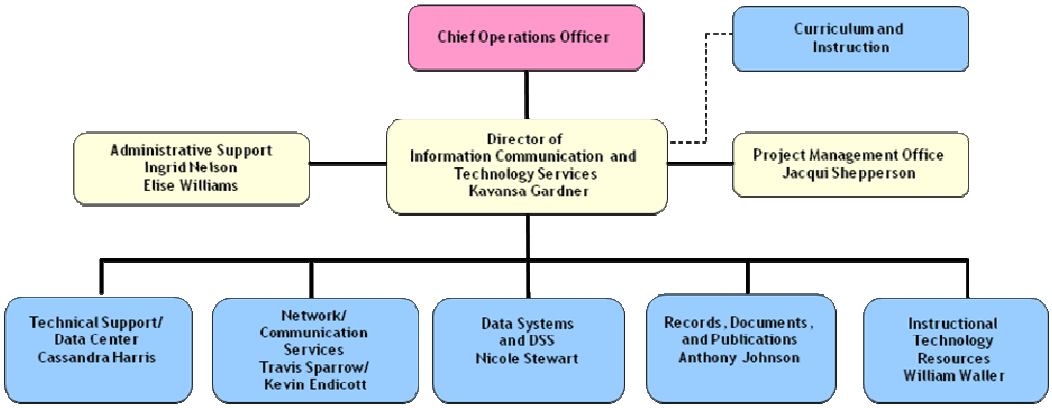


Figure 3. Organizational Chart for Information Communication and Technology Services

The individual groups are described in the following sections.

5.1 Project Management Office

The Project Management Office is a new group in ICTS. With a number of major initiatives underway, all of which impact multiple departments within the district, it is critical that they be coordinated and managed effectively in order to ensure a seamless implementation. The Project Management Office is staffed by a Program Manager, who is responsible for overseeing the smooth implementation of all initiatives and managing interdependencies between them, a project manager, who is responsible for managing one or more individual projects, a project coordinator who facilitates project scheduling and task management, and a business analyst, who assists with the management of project budgets, purchase orders, etc. Figure 4 shows the organization of the Project Management Office.

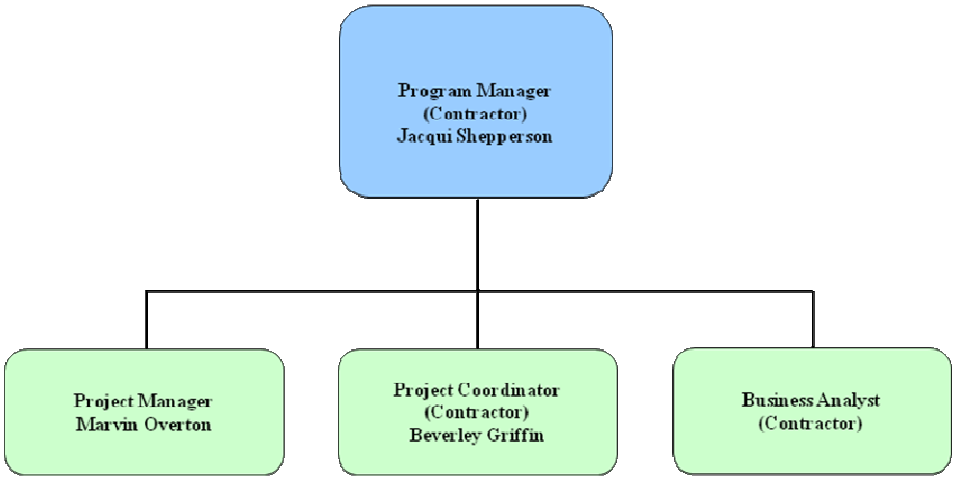


Figure 4. Project Management Office

5.2 Technical Support/Data Center

DIT's Computer Services Center and Data Support Center will combine to form the Technical Support/Data Center. Because users do not differentiate between desktop issues and server issues when making a request for help, it makes sense for these groups to be combined. The new Help Desk, which will provide an increased level of telephone support to most users, will cement this relationship and manage Remedy, provide initial troubleshooting support, create an FAQ for users, screening calls to reduce the dependency on site visits. This group will consist of the 4 FTE from the Data Center, the 12 FTE from Computer Services, the Technology Asset Administrator, and the 3 FTE from the Help Desk. Figure 5 shows the organization of the Technical Support/Data Center group.

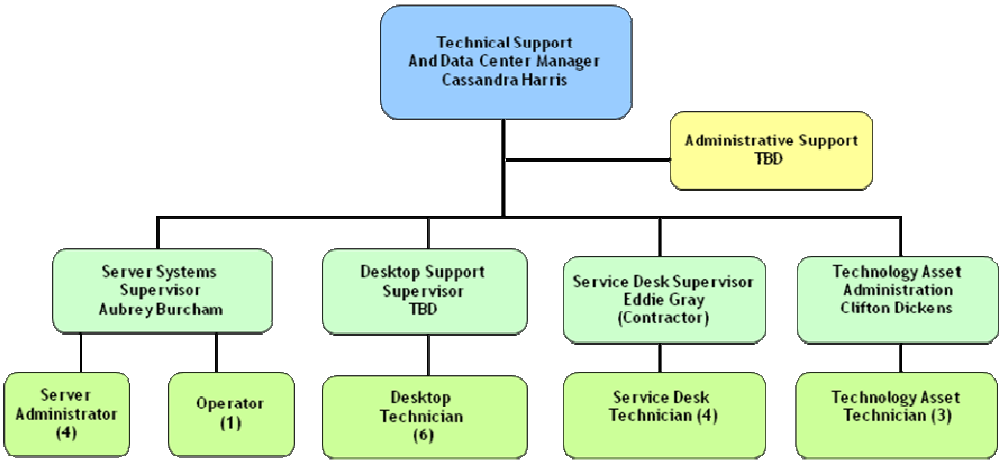


Figure 5. Technical Support/Data Center Group

5.3 Network/Communications Services

DIT's Network Operations staff and the Office of Telecommunications staff will combine to form the Network/Communication Services group. As telephone and Internet services share wiring and potentially bandwidth, these services should be synchronized and managed with the E-Rate oversight that provides significant funding for these efforts. This group will consist of the 2 FTE from Network Operations and the 7 technical FTE from Telecommunications. Figure 6 shows the organization of the Network/Communication Services Group.

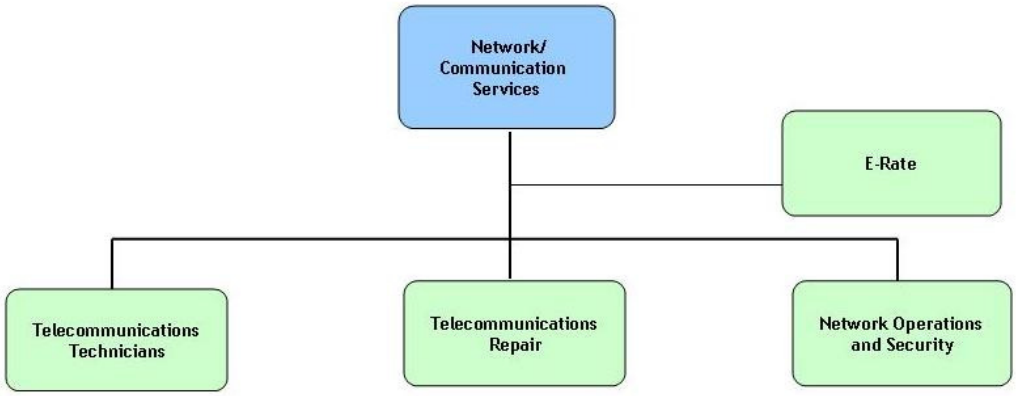


Figure 6. Network/Communications Services Group

5.4 Data Systems/Decision Support Services

DIT's Data Systems and Reporting Group remain functionally the same, but will be renamed the Data Systems/Decision Support Services group. The focus of this group will be maintaining the current systems as well as implementing a comprehensive data governance project as a prelude to the data warehouse project. This group will consist of the 10.5 FTE from the current Data Systems group Figure 7 shows the organization of the Data Systems/Decision Support Services group.

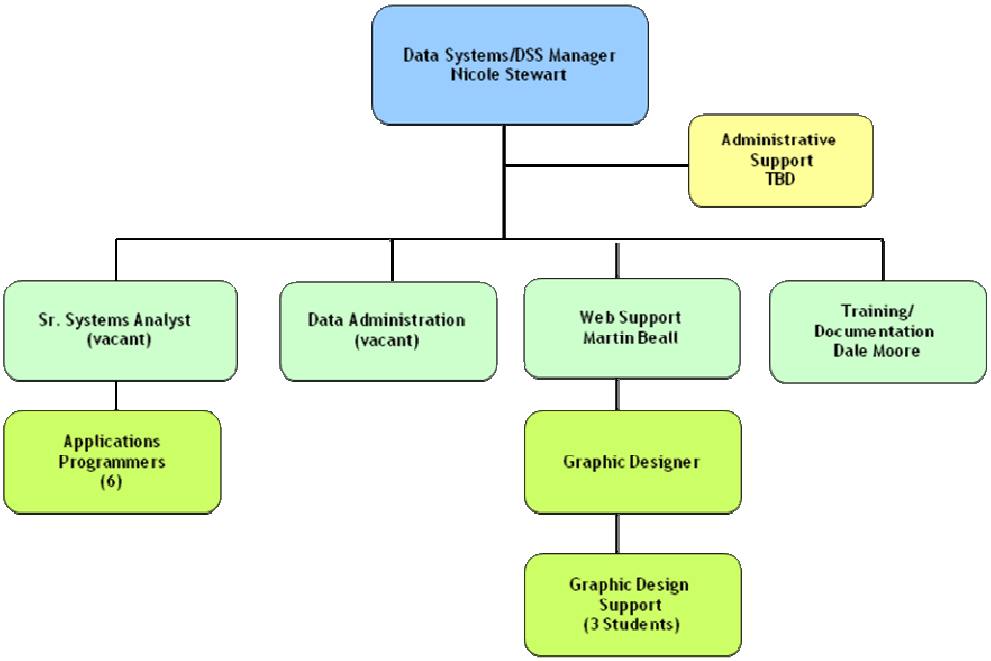


Figure 7. Data Systems/Decision Support Services

5.5 Records, Documents, and Publications Services

DIT's Records Management Division Center will expand its services to become the Records, Documents, and Publications Group. In addition to scanning student and employee records, this group will be responsible for managing the new centralized print shop and for archiving the myriad documents within the district, including policies, procedures, and other documents that must be managed.

(Note: It is recommended that the other copy centers operated by RPS, including those at City Hall, which are not currently run though this group, be consolidated into a single operation when practicable.)

This group will consist of the 4.5 FTE existing group plus an additional FTE for the copy center. Figure 8 shows the organization of the Records, Documents, and Publications Services group.

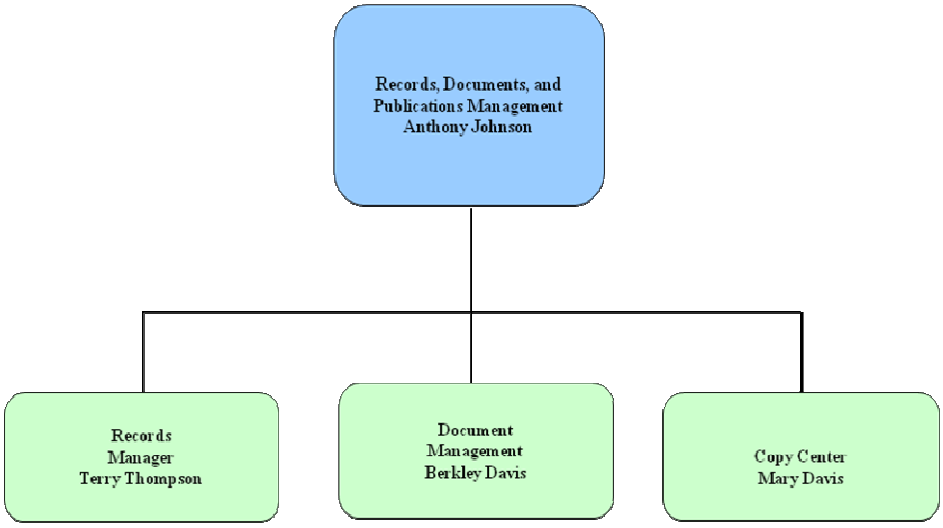


Figure 8. Records, Documents, and Publications Services Group

5.6 Instructional Technology Resources

As a long-term goal, the Information Communication and Technology Services department should oversee the Instructional Technology Resource Teachers. It is important that the vision for instructional technology in the district be developed and implemented collaboratively by all of the key stakeholders in this area. While these individuals are physically located in the schools, it is important for them to coordinate closely with each other and with others in ICTS. By providing an organizational home for the ITRTs, they will be able to collaborate on professional development, resources, and best practices, resulting in a stronger group that can best serve the district. This group would also include ICTS' Applications Trainers, enabling them to provide a greater level of user training and to address some of this in the context of curriculum integration training.

Until that change is feasible, the Instructional Technology Resources group will continue to be the liaison between the ICTS and the Curriculum and Instruction group, as shown in Figure 9.

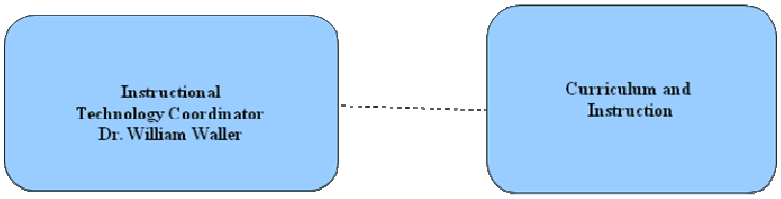


Figure 9. Instructional Technology Resources Group

Appendix A: Job Descriptions

Add Job Description for

Telecommunications positions

Administrative Accountant – Business analyst

Records, Documents & Publications Manager

Trainers

Comment [KG2]: Insert TRAINERS

Job Description for Director
Information Communication and Technology Services

Goal	Manages and directs the district toward its primary technological objectives, based on long-term product and profitability goals, by performing the following duties personally or through subordinate managers.
Performance Responsibilities	Provides for telecommunications, network operations and computer repair center operations, and district-wide technology training. Establishes, plans, and directs the organization's IT architecture, standards, design frameworks, procurement approaches, implementation/operation policies, and monitoring/maintenance strategies. Reports to the administration on the progress in electronic data management, processing and storage projects, resource utilization, and production performance. Serves as the Superintendent's representative for administrative management of electronic information management, processing and storage Reviews and monitors adherence to consistent, state-of-the-art technical architectural standards for all products and services. Oversees and coordinates internal information technology function as well as system access and security. Creates a technical vision for the company and plans for implementation of new technical projects or product lines. Creates technical budgets, allocates resources, and determines schedule of product releases or project deadlines. Establishes and maintains an effective system of electronic communications throughout the organization. Analyzes new technologies and runs competitive analyses. Develops and oversees a fixed asset and human resources program for keeping all information technology resources current and state-of-the-art. Develops requests or proposals as necessary to procure project deliverables. Performs other related duties as assigned.
Education	Bachelor's Degree required in Computer Science, Information Systems or relevant discipline. Master's Degree in a related area preferred.
Qualifications	Exceptional communication and public relations skills along with executive level research, staff and organizational development and strategic planning skills are a necessity. Must have a comprehensive knowledge and extensive hands-on experience with the principles, practices, techniques to successfully lead and manage an IT department with a $15 million budget and 52 full and part-time personnel. Must possess the ability to effectively manage and supervise the full range of IT services for over 65 locations with over 14,000 computers and other related hardware to maintain fully operational. Demonstrated leadership and management skills with a proven track record of success with solving complex technology problems. Must have extensive experience managing systems and applications development, computer maintenance and repair programs, and staff development.

Job Description for Director
Information Communication and Technology Services

Qualifications (cont'd)	Some experience with technology grants preferred. Excellent organizational and presentation skills, ability to work independently and implement effective decision making skills required. Must have the ability to establish and maintain effective working relationships with administrators, school staff, supervisors, managers, technicians, and other employees. Must have the ability to develop and implement financial management and accounting controls of program expenditures.
Pay Scale	Twelve-month contract position ; Grade 19, FLSA: Exempt
Experience	A minimum of five years of recent successful administrative management experience supervising the operations of an IT department for a large urban public school system as Senior Director, Director, Assistant Director or an equivalent administrative position.
Reports to:	Chief Operating Officer
Supervises:	ICTS Department
Last Revised	July 14, 2008

Job Description for IT Program Manager
Information Communication and Technology Services

Goal	Oversees the delivery of projects to an acceptable level of risk by balancing scope, time, cost and quality. Plans, organizes and coordinates all IT projects, to ensure they are strategically aligned to the mission and goals of RPS and implemented on time, within budget, and with minimal disruption to RPS day-to-day business and activities.
Performance Responsibilities	Monitors status of all projects and interdependencies. Maintains issues-resolution file to ensure that all issues are addressed. Oversees the development and tracking of integrated project plans; Adapts and applies the ITIL delivery approach to meet project objectives and RPS business drivers; establishes and maintains project communications. Oversees project estimations and the development of project deliverables. Manages project managers and coordinators to assure processes are manageable through the project lifecycle. Partners with others to lead teams; builds and structures project teams to ensure maximum performance; provides purpose, direction and motivation to team; clarifies and communicates project objectives and success criteria; ensures a positive, collaborative work environment. Meets with RPS department and cabinet members as needed and provides appropriate and timely communication throughout the life of projects using reports, team meeting notes, dashboards, Gantt charts, etc. Directly supervises the work of associate Project Manager(s) and third-party partner and/or vendor relationships, as necessary. Develops and maintains relationships with key business stakeholders to ensure deliverables are effective.
Education	Bachelor's degree from an accredited four-year college or university required; Masters preferred. Project Management Professional Certification (PMI).
Qualifications	Strong familiarity with or certification in Information Technology Infrastructure Library of Best Practices preferred. 1-2 years of client management experience with primary accountability for peer-level client relationships, and experienced multiple full project lifecycles from business development to final delivery; Broad technical background with exceptional planning, coordinating, management, communication and presentation skills. Demonstrated leadership and project management skills with proven track record of success with large-scale enterprise technology projects. Experience managing technology grants and/or Information Technology (IT) applications development preferred. Experience using object-oriented design and development methodologies preferred. Proficient in MS Project, Outlook, Word, Excel, PowerPoint, and Visio. Must be able to plan and manage work in a team environment.
Other Qualifications	Excellent organizational skills, ability to work independently and implement effective decision making skills toward completion of assigned tasks. Ability to work under pressure and meet multiple deadlines. Ability to establish and maintain effective professional working relationships and work in a cooperative and collaborative manner with administrators, supervisors, managers, technicians and other employees.
Pay Scale	Twelve-month position, Pay grade 18, FLSA: Exempt
Experience	A minimum of two years' project management experience is required.

Reports to	Director, ICTS
Supervises:	
Last Revised	July 26, 2008

Job Description for IT Project Manager
Information Communication and Technology Services

Goal	Primary goal of this position is to plan and manage the delivery of business systems solutions in support of business objectives and ongoing operations.
Performance Responsibilities	Manages project planning, estimating, execution, implementation and ongoing support. Works closely with functional business groups to ensure the efficiency and effectiveness of projects; identifies needed resources, assigns responsibilities, monitors performance, resolves conflicts and motivates team members. Responsible for gathering project scopes, statements of work, status information and providing guidance to the project team on deliverables, expectations, responsibilities and overall accountabilities. Develops and manages all appropriate project management documents including, but not limited to, project charter, plan, and timelines. Works cohesively with Program Manager to facilitate in the dissemination of appropriate communication throughout the lifecycle of projects. Conducts scheduled project team meetings to gather and compile project status information and provide tasks, information and guidance to the project team members. Effectively collaborates with team to assure all tasks are properly tasked and any issues, risks, deliverables and communication plans are properly documented throughout the project lifecycle. Provides timely communication through the development and maintenance of project reports, team meeting agendas and meeting minutes; Dashboards and Gantt charts, etc. Manages service delivery and overall performance by effectively collaborating with other business units. Performs other related duties as assigned.
Education	Bachelor's degree from an accredited four-year college or university; Project Management Professional Certification (PMI) and strong functional working knowledge in Information Technology and Information Library (ITIL-foundational) framework.
Qualifications	Must be an effective communicator (orally and in writing), with a willingness to share and work well with others. Broad technical background with exceptional planning, coordinating, management, communication and presentation skills. Demonstrated project management skills with proven skills to effectively manage, implement, and document projects. . Experience managing technology grants and/or Information Technology (IT) applications development preferred. Proficiency in Microsoft 2007 products, including Microsoft Project, Visio, Outlook, Word, Excel, and PowerPoint. Must be able to plan and manage work in a team environment.
Other Qualifications	Excellent organizational skills, ability to work independently and implement effective decision making skills toward completion of assigned tasks. Ability to work under pressure and meet multiple deadlines. Ability to establish and maintain effective professional working relationships and work in a cooperative and collaborative manner with administrators, supervisors, managers, technicians and other employees.
Pay Scale	Twelve-month position, Pay grade 17 FLSA: Exempt
Experience	A minimum of two years' project management experience is required.

Reports to	Program Manager, ICTS
Supervises:	
Last Revised	July 14, 2008

Job Description for IT Project Coordinator
Information Communication and Technology Services

Goal	Responsible for coordinating and completing multiple projects simultaneously. Oversees all aspects of projects including, but not limited to setting deadlines, assigning responsibilities and summarizing the progress of projects maintained.
Performance Responsibilities	Works with Program and Project Managers to assure the coordination of project teams and identifies needed resources to accomplish tasks in a timely manner. Requires a wide degree of creativity and customer service skills. Develops and manages all applicable project documentation including, but not limited to: project plans, charters, emails, meetings, calendars and documentation. Must-attend team meetings regularly to assure project status information and timeliness are effectively communicated and assists project team members by providing information and guidance when needed. Provides appropriate and timely communication throughout the lifecycle of projects through the use and development of reports, team meeting agendas and the coordination for the delivery of status reports, timelines, project budgets and estimates~~,~~ Apprises Project Managers and Program Managers of potential obstacles to on time/within budget completion.
Education	Associates' Degree required in Computer Science, Information Systems or relevant discipline. Bachelor's degree preferred. Project Management Certification preferred. Working knowledge of Project Management Methodology and ITIL Framework.
Qualifications	Broad technical background with exceptional planning, coordinating, management, communication and presentation skills. Demonstrated leadership and project management skills with a proven track record of success with complex technology projects. Experience managing technology grants and/or Information Technology (IT) applications development preferred. Proficiency in MS Project, Word, Excel, Outlook and PowerPoint. Must be able to plan and manage work in a team environment.
Other Qualifications	Excellent organizational skills, ability to work independently and implement effective decision making skills toward completion of assigned tasks. Ability to work under pressure and meet multiple deadlines. Ability to establish and maintain effective professional working relationships and work in a cooperative and collaborative manner with administrators, supervisors, managers, technicians and other employees.
Pay Scale	Twelve-month position, Pay grade 15
Experience	A minimum of six months' project coordination experience is required.
Reports to	Program Manager, ICTS
Supervises:	
Last Revised	July 26, 2008

Job Description for Business Analyst
Information Communication and Technology Services

Goal	Plans, organizes and coordinates all aspects of an IT project, ensuring that the goals and objectives of the project are accomplished on time and within budget.
Performance Responsibilities	Maintain project budgets for all IT projects. Complete and submit purchase orders for managed projects. Confirm receipt of orders and process invoices. Coordinate billing as appropriate. Facilitate development of RFP's. Maintain tracking of RFP's Other duties as assigned.
Education	High School diploma required. Associates degree in business preferred.
Qualifications	Broad technical background with exceptional planning, coordinating, management, communication and presentation skills. A proven track record of success with complex technology projects. Proficiency in MS Project, Word, Excel, and PowerPoint. Must be able to plan and manage work in a team environment.
Other Qualifications	Excellent organizational skills, ability to work independently and implement effective decision making skills toward completion of assigned tasks. Ability to work under pressure and meet multiple deadlines. Ability to establish and maintain effective professional working relationships and work in a cooperative and collaborative manner with administrators, supervisors, managers, technicians and other employees.
Pay Scale	Twelve-month position, Pay grade 16, FLSA: Exempt
Experience	A minimum of six months' business experience with bookkeeping preferred. .
Reports to	Program manager, ICTS
Supervises:	
Last Revised	July 26, 2008

Job Description for Administrative Assistant
Information Communication and Technology Services

Goal	Plans, initiates, and carries to completion office support activities for the Department of Information Communication and Technology Services
Performance Responsibilities	Maintains logs on incoming telephone calls, correspondence and action documents, and follows up on work in progress to ensure timely response or action. Maintains supervisor's calendar as required, formats and types confidential and general correspondence, reports, and statistical data. Tabulates and prepares reports of financial data, and makes travel arrangements. Operates a personal computer and related equipment to produce correspondence, reports, charts and other materials using numerous management techniques to enter, edit, print and file data. Maintains all leaves, payroll, and personnel records, clerical records and reports. Greets customers in person or on the telephone; answering or referring inquiries. Maintains customer confidence and protects operations by keeping information confidential. Maintains office supplies by checking stock to determine inventory levels, anticipating needed supplies; placing and expediting orders. Keeps equipment operational by following manufacturer's instructions and procedures. Secures information by completing database backups. Provides historical reference by utilizing filing and retrieval systems. Maintains technical knowledge by attending educational workshops and reading administrative support publications. Performs other related duties as assigned
Education	High school diploma is required.
Qualifications	Must have a general knowledge of business office procedures, practices, and equipment and the ability to quickly learn operations of the office and other duties as assigned. Must be skilled at mathematical calculations and demonstrate excellence in business English, grammar, spelling, and punctuation. Excellent communication, organizational, and public relations skills required. Excellent computer skills are required. Must be able to demonstrate proficiency in Microsoft Word, Excel, Access and PowerPoint, as well as all aspects of Outlook.
Other Qualifications	Must be able to establish and maintain effective working relationships with others and be adaptable to changing priorities. The ability to efficiently organize assignments, effectively handle multiple assignments simultaneously, and work effectively under minimum or no supervision is essential. Must have the ability to exercise tact, good judgment and demonstrate initiative in the completion of assignments.
Pay Scale	Twelve month contract, Pay grade 10, FLSA: Exempt

Comment [KG3]: Delete ??? add 10

Job Description for Administrative Assistant
Information Communication and Technology Services

Experience	A minimum of one year office experience is required.
Reports to:	Director of Information Communication and Technology Services
Supervises:	NA
Last Revised	July 14, 2008

Job Description for Data Center and Technical Support Manager
Information Communication and Technology Services

Goal	Coordinates the use of resources for the Server/ Data Center, Desktop Asset Management and Service Desk. Oversees daily operations and major projects at Network Operations Center and Technical Support Center, including server administration, technical support, asset management, and Help Desk.
Performance Responsibilities	Work with Director of ICTS to plan and implement major project related to server administration and technical support. Forming emergency response teams to correct wide scale problems: malicious attacks, worms, virus, spyware, etc. Prepares and receives requests for Request for Proposals (RFP). Knowledge of Power, Cooling and Facilities Engineering inside a Data Center. Must have a demonstrated ability to successfully manage all aspects of change to the computing infrastructure and problems that arise to maximize system availability and reliability while minimizing risks. Provides the development and maintenance of technological roadmaps for represented areas. Monitors the ongoing work of the network operations center. Monitors the help desk call tracking system, including call assignments, follow-up and the generation of reports for the department Manager. Provides technical support and assistance to schools and departments in the selection, installation, operation, and maintenance of computer hardware and software. Prepares reports as required. Coordinates with instructional and administrative personnel on networked software needs of a school or department. Participates in the development and publication of technology standards. Assists the Director, Information Technologies in planning and development of the technology budget. Performs administrative duties, including ordering and returning pans and processing vendor invoices. Performs other duties as assigned.
Education	Bachelor's Degree in Computer Information Systems. Masters Degree in Information Technology, Computer Science or other related discipline mandatory.
Qualifications	Certification (A+, Apple and Compaq) preferred. Must have consistent knowledge of changing technology to facilitate visionary planning for collective system. Must have at least 4 years of experience managing a technology Data Center environment. Be passionate about the quality and quantity of services being provided by the Data Center Operation team and always strive to improve the overall customer experience. Skill in analyzing and solving hardware and software problems related to compatibility networking and configuration issues.

	Must have strong leadership, organizational and administrative skills. Ability to excel in a customer service-driven environment. Knowledge of LAN and WAN environments. Must possess interpersonal skills in working with users, vendors and general public.
Other Qualifications	NA
Pay Scale	Twelve-month position ; Pay Grade 21, FLSA: Exempt
Experience	At least 6years of experience in a networked information systems environment.
Reports to	Director, ICTS
Supervises	
Last Revised	July 14, 2008 (Prev. rev December 8, 2000)

Job Description for Server Systems Supervisor
Information Communication and Technology Services

Goal	Oversees daily operations and major projects at Network Operations Center and supervises Server Technicians and Operator.
Performance Responsibilities	Work with Technical Support and Data Center Manager to plan and implement major projects related to server administration. Monitors the ongoing work of the network operations center. Responds to support problems with NOC on evenings/weekends when required. Manages the deployment process of software updates and patches. Provides timely status documentation for system compliancy. Works closely with programming staff to coordinate software implementations. Provides reporting on status of server system availability, health and growth needs. Develops procedural documentation for standard operating procedures. Installs, troubleshoots and configures hardware server equipment. Troubleshoots problems with servers and makes necessary repairs and adjustments. Develops and maintains a maintenance schedule for servers including upgrade or replacement of hardware and software. Ensures that all software patches are applied in a timely manner. Develops tape backup and rotation procedures at the server level. Develops and communicates a server-level security policy. Ensures appropriate access controls are in place. Prepares and receives Requests For Proposals (RFP) concerning servers, networks and related equipment and actively participates in the vendor selection. Participates in the development and publication of technology standards. Assists data Center Manager in developing the technology budget. Performs other related duties as assigned.
Education	Must have Bachelor's Degree. Computer Information Systems or Computer Science discipline preferred
Qualifications	MCSE certification preferred. Experience in Novell open enterprise server administration. Experience managing large scale server environment in excess of 100 units. Experience with virtual server technology (2-3 years). Skill in analyzing and solving hardware and software problems related to compatibility networking and configuration issues. Must have strong leadership, organizational and administrative skills. Ability to excel in a customer service-driven environment. In-depth Knowledge of LAN and WAN environments. Must possess interpersonal skills in working with users, vendors and general public. Must have knowledge of data center power management.
Other Qualifications	NA
Pay Scale	Twelve-month position ; Pay Grade 18 FLSA: Exempt

Experience	At least 5 years of experience in a networked information systems environment.
Reports to	Technical Support and Data Center Manager, ICTS
Supervises	
Last Revised	July 26, 2008

Job Description for Server Administrator
Information Communication and Technology Services

Goal	Installs, configures and, maintains Windows and Novell servers in Richmond Public Schools and departments.
Performance Responsibilities	Troubleshoots problems with servers and makes necessary repairs and adjustments. Works in close collaboration with Desktop supervisor for planning of all client/server and web-based implementation. Experience in Novell Open Enterprise Server environment. Experience in Iseries, AS400 administration. Performs network administration including installing software and setting up user accounts, share directories and print queues. Develops and maintains a maintenance schedule for servers including upgrade or replacement of hardware and software. Ensures that all software patches are applied in a timely manner. Administers tape backup and rotation procedures at the server level. Assists in the development, publication and maintenance of a disaster recovery plan. Performs other related duties as assigned.
Education	Bachelors' degree in Computer Science, Information Systems or a related field preferred.
Qualifications	MCSE certification preferred. Must possess an excellent working knowledge of tape backup and virus protection software. Must have excellent oral and written communication skills and the ability to work well with people at all levels of the organization. Must be able to handle multiple projects and requests for assistance in an organized manner with little or no supervision. Must have excellent public relation skills, excellent "customer service" attitude and a positive work ethic.
Other Qualifications	Must have a valid Virginia Motor Vehicle operators' license, evidence of a good driving record and be willing to use your personal vehicle to travel locally to schools and departments.
Pay Scale	Twelve-month position ; Pay Grade 17, FLSA: Exempt
Experience	Must have a minimum of 4 years of progressively responsible experience as a Microsoft network administrator.
Reports to:	Server Systems Supervisor
Supervises	
Last Revised	June 25, 2008 (previous rev. 8/5/04)

Job Description for Server Operator
Information Communication and Technology Services

Goal	TBD.
Performance Responsibilities	TBD.
Education	TBD
Qualifications	TBD
Other Qualifications	TBD
Pay Scale	Twelve-month position ; Pay Grade ???, FLSA: Exempt
Experience	TBD
Reports to:	Server Systems Supervisor of ICTS
Supervises	
Last Revised	July 29, 2008

Job Description for Desktop Support Supervisor
Information Communication and Technology Services

Goal	Coordinates district-wide technical support and maintenance work, including preventive and corrective maintenance on computer equipment and associated peripherals; does related work as required.
Performance Responsibilities	Serves as dispatcher to ensure that all calls are handled in a timely fashion. Coordinates the installation and configuration of computers and printers in network environments throughout the district Must make routine visits to schools; communicate with Principals on the perceived service level being offered by group. Maintains reporting on the efficient use of allocation for the support staff. Works in close collaboration with server system supervisor for planning of all client/server and web-based implementation. Handles multiple projects efficiently within deadlines while ensuring quality outcome. Maintains appropriate written documentation for new installations and upgrades. Addresses service-related issues between the desktop technicians and the central office or school-sites. Coordinates off-site maintenance and repair of computers and printers with vendors. Recommends procedures for backup of computers and servers. Uses own personal vehicle for travel to various Richmond Public School work sites. Performs other related duties as assigned.
Education	Associate's Degree in Computer Science, Information Systems or a related field is preferred.
Qualifications	Must have demonstrated ability to perform repairs and upgrades to microcomputers. HP, A+ and Macintosh certifications are preferred. Novell and Microsoft experience is preferred. Must be able to work with vendors and to develop documentation and training records. Must have good leadership skills and strong team-building ability. Must have a positive work ethic; possess excellent communications and public relations skills along with excellent customer service and organizational/planning skills. Must be able to work independently with minimum supervision, adaptable to changing priorities, effectively manage and complete multiple assignments within deadlines. Must be able to communicate efficiently in technical or simple terms as appropriate to end users, staff, and management. Must have the personality and ability to establish and maintain professional working relationships with school staff, employees, and other customers.
Other Qualifications	Must have a valid Virginia Motor Vehicle Operators license and evidence of good driving record. Must be willing to use own personal vehicle for some required local travel.
Other Qualifications (cont'd)	Vocal communication is required for expressing or exchanging ideas by means of the spoken word, and conveying detailed or important instructions to others accurately, loudly, or quickly.

Job Description for Desktop Support Supervisor
Information Communication and Technology Services

	Hearing is required to perceive information at normal spoken word levels, and to receive detailed information through oral communications and/or to make fine distinctions in sound. Visual acuity is required for depth perception, color perception, preparing and analyzing written or computer data, visual inspection involving small defects and/or small parts, use of measuring devices, assembly or fabrication of parts at or within arms length, operation of machines, operation of motor vehicles or equipment, determining the accuracy and thoroughness of work, and observing general surroundings and activities. The worker is subject to inside and outside environmental conditions, hazards, and atmospheric conditions.
Pay Scale	Twelve-months ; Pay grade 15 FLSA: Non-exempt
Experience	Must have a minimum of 3years experience in the installation, setup, and maintenance of computers in a networked environment.
Reports to:	Manager, Technical Support and Data Center
Supervises:	Desktop Technicians
Last Revised	July 26, 2008

Job Description for Desktop Technician
Information Communication and Technology Services

Goal	Performs responsible technical work performing preventive and corrective maintenance on computer equipment and associated peripherals; does related work as required.
Performance Responsibilities	Sets up, configures, and troubleshoots computers and printers in a network environment. Handles multiple projects efficiently within deadlines while ensuring quality outcome. Installs software on desktop and laptops. Must be willing to be notified via GPS tracking system technology for efficient use resources. Maintains appropriate written documentation for new installations and upgrades. Conducts minor repairs and upgrades of computers including, but not limited to the installation of network cards, modems, and memory. Analyzes and resolves hardware, software, and networking problems. Recommends procedures for backup of computers and servers. Uses own personal vehicle for travel to various Richmond Public School work sites. Performs other related duties as assigned.
Education	Associate's Degree in Computer Science, Information Systems or a related field is preferred.
Qualifications	Novell and Microsoft experience is preferred. Must have demonstrated ability to perform repairs and upgrades to microcomputers. Compaq, A+, and Macintosh certifications are preferred. Must be able to work with vendors and to develop documentation and training records. Must have a positive work ethic; possess excellent communications and public relations skills along with excellent customer service and organizational/planning skills. Must be able to work independently with minimum supervision, adaptable to changing priorities, effectively manage and complete multiple assignments within deadlines. Must be able to communicate efficiently in technical or simple terms as appropriate to end users, staff, and management. Must have the personality and ability to establish and maintain professional working relationships with school staff, employees, and other customers.
Other Qualifications	Must have a valid Virginia Motor Vehicle Operators license and evidence of good driving record. Must be willing to use own personal vehicle for some required local travel. Work is performed under regular supervision. This is medium work requiring the exertion of 50 pounds of force occasionally, up to 20 pounds of force frequently, and up to 10 pounds of force constantly to move objects; work requires climbing, balancing, stooping, kneeling, crouching, crawling, reaching, standing, walking, pushing, pulling, lifting, fingering, grasping, feeling, and repetitive motions.
Other Qualifications	Vocal communication is required for expressing or exchanging ideas by means of the spoken word, and conveying detailed or important instructions to others

Job Description for Desktop Technician
Information Communication and Technology Services

(cont'd)	accurately, loudly, or quickly. Hearing is required to perceive information at normal spoken word levels, and to receive detailed information through oral communications and/or to make fine distinctions in sound. Visual acuity is required for depth perception, color perception, preparing and analyzing written or computer data, visual inspection involving small defects and/or small parts, use of measuring devices, assembly or fabrication of parts at or within arms length, operation of machines, operation of motor vehicles or equipment, determining the accuracy and thoroughness of work, and observing general surroundings and activities. The worker is subject to inside and outside environmental conditions, hazards, and atmospheric conditions.
Pay Scale	Twelve-months ; Pay grade 11, FLSA: Non-exempt
Experience	Must have a minimum of 2 years experience in the installation, setup, and maintenance of computers in a networked environment.
Reports to:	Supervisor, Desktop Support
Supervises:	NA
Last Revised	July 14, 2008

Job Description for Service Desk Supervisor
Information Communication and Technology Services

Goal	Supervises Service Desk technicians and oversees service desk operations. Define and document procedures for operating and maintaining telephone service center. Works in close collaboration with Desktop Supervisor.
Performance Responsibilities	Provide customer service to all end-users in a prompt, professional and courteous manner. Evaluate, prioritize and schedule problem resolutions; escalate problem resolutions (when required) to the appropriately experienced technician. Identify mass computer related outages (power, network and server). Notify technicians of current state, estimated time of resolution and resolution details. . Works closely with training staff to identify training needs. Monitors the perceived documented efficiency and customer service of the service center. Must have ITIL knowledge of best practices. Develops Service Desk documentation for all standard operating procedures. Test, evaluate and coordinate presentation of proposed software applications.. Provide reporting of computer and related item assets. Design, develop and maintain website and changes to website. Manage CIMS job queue. Provide test environment for programmatic changes. Maintain documentation of programmatic changes. Track and report server and network (to include wireless access) monitoring. Trends and downtime. Provide hardware and application standards. Provide input and generate IT Policies and Procedures where necessary. Perform other duties as assigned.
Education	Associate's Degree in Computer Science, Information Systems or a related field is preferred.
Qualifications	. Must have Windows experience, Novell experience desired. Must have remote desktop management experience with Altiris of LANDesk software. Must have experience in helpdesk software management platforms. Demonstrated ability to perform repairs and upgrades to desktop systems. A+ certification is required, CNE certification is preferred. Must be able to work with vendors and to develop documentation and training records. Must have a positive work ethic; possess excellent communications and public relations skills along with excellent customer service and organizational/planning skills. Must be able to communicate efficiently in technical or simple terms as appropriate to end users, staff, and management. Must have good leadership skills and the ability to establish and maintain professional working relationships with others.

Job Description for Service Desk Supervisor
Information Communication and Technology Services

Pay Scale	Twelve-months ; Pay grade15, FLSA: Non-exempt
Experience	Must have a minimum of 3 years in desktop support.
Reports to:	Manager, Data Center and Technical Support
Supervises:	Service Desk Technicians
Last Revised	July 26 2008

Job Description for Service Desk Technician
Information Communication and Technology Services

Goal	Performs responsible technical support via telephone and assist with documenting maintenance and troubleshooting procedures.
Performance Responsibilities	Provide customer service to all end-users in a prompt, professional and courteous manner. Field incoming help requests from end-users via telephone, e-mail and in person. Instill a feeling of confidence in end-users regarding the Department of Information Technology by building a rapport with help desk customers. Document all pertinent end-user identification information in the automated Help Desk tracking system, including (but not limited to): name, department, contact information, nature of problem, time, date and any details mentioned. Escalate calls to appropriate Tiers II or III if call is of Severity 1 or 2 or VIP status. Verify/ensure minimum desktop configuration in place for end-user. Provide additional updates if necessary, in addition to issue at hand. Apply diagnostic utilities to aid in troubleshooting. Perform hands-on fixes at the desktop level, including installing and upgrading software, implementing file backups, and configuring systems and applications utilizing the Desktop Management tool. Test fixes to ensure problem resolution is appropriate and adequate for logged issue. Access software updates, drivers, knowledge bases, and frequently asked questions resources via the Internet to aid in problem resolution. Provide Password Self Service assistance/training for Single-Sign on Performs other related duties as assigned.
Education	Associate's Degree in Computer Science, Information Systems or a related field is preferred.
Qualifications	Novell and Microsoft experience is preferred. Must have demonstrated ability to perform repairs and upgrades to microcomputers. HP, A+, and Macintosh certifications are preferred. Must be able to work with vendors and to develop documentation and training records. Must have a positive work ethic; possess excellent communications and public relations skills along with excellent customer service and organizational/planning skills. Must be able to work independently with minimum supervision, adaptable to changing priorities, effectively manage and complete multiple assignments within deadlines. Must be able to communicate efficiently in technical or simple terms as appropriate to end users, staff, and management. Must have the personality and ability to establish and maintain professional working relationships with school staff, employees, and other customers.

Job Description for Service Desk Technician
Information Communication and Technology Services

Other Qualifications	Must have a valid Virginia Motor Vehicle Operators license and evidence of good driving record. Vocal communication is required for expressing or exchanging ideas by means of the spoken word, and conveying detailed or important instructions to others accurately, loudly, or quickly. Hearing is required to perceive information at normal spoken word levels, and to receive detailed information through oral communications and/or to make fine distinctions in sound. Visual acuity is required for depth perception, color perception, preparing and analyzing written or computer data, visual inspection involving small defects and/or small parts, use of measuring devices, assembly or fabrication of parts at or within arms length, operation of machines, operation of motor vehicles or equipment, determining the accuracy and thoroughness of work, and observing general surroundings and activities. The worker is subject to inside and outside environmental conditions, hazards, and atmospheric conditions.
Pay Scale	Twelve-months ; Pay grade 11, FLSA: Non-exempt
Experience	Must have a minimum of 2 years experience in the installation, setup, and maintenance of computers in a networked environment.
Reports to:	Supervisor, Service Desk
Supervises:	NA
Last Revised	July 14, 2008

Job Description for Technology Asset Administration Information Communication and Technology Services

Goal	TBD.
Performance Responsibilities	TBD.
Education	TBD
Qualifications	TBD
Other Qualifications	TBD
Pay Scale	Twelve-month position ; Pay Grade ???, FLSA: Exempt
Experience	TBD
Reports to:	Server Systems Supervisor of ICTS
Supervises	
Last Revised	July 29, 2008

Job Description for Technology Asset Technician
Information Communication and Technology Services

Goal	TBD.
Performance Responsibilities	TBD.
Education	TBD
Qualifications	TBD
Other Qualifications	TBD
Pay Scale	Twelve-month position ; Pay Grade ???, FLSA: Exempt
Experience	TBD
Reports to:	Server Systems Supervisor of ICTS
Supervises	
Last Revised	July 29, 2008

Job Description for Data Systems/DSS Supervisor
Information Communication and Technology Services

Goal	Coordinates and monitors the development and maintenance of all administrative/business applications of the school division.
Performance Responsibilities	Works closely with users to gather information, clarify system objectives and resolve problems. Provides programming support and technical guidance to the application programmers. Evaluates new systems and applications and presents formal recommendations. Serves as database administrator. Develops and enforces programming and database policies, procedures and standards to ensure integration and maximum performance of systems and applications. Oversees the installation of software patches, fixes and version upgrades and new installations. Prepares and receives Requests for Proposals (RFP). Assists with vendor selection. Assists in the planning and development of the technology budget. Assists in the development and maintenance of a disaster recovery plan. Performs other related duties as assigned.
Education	Bachelors' degree required in Computer Science, Information Systems or related field.
Qualifications	Proficiency in RPG/400 programming required. Experience with SQL and Oracle databases preferred. Programming experience in C++, Visual Basic and SAS desirable. Experience with K-12 education applications highly desirable. Project development and management experience required. Excellent analytical and problem-solving abilities required. Must have the ability to work well with people in all levels of the organization. Must be able to handle multiple projects and requests for assistance in an organized manner with little or no supervision. Must have excellent public relations skills, excellent "customer service" attitude and positive work ethic.
Other Qualifications	Must have a valid Virginia Motor Vehicle operators' license and be able to travel locally to schools and departments.
Pay Scale	Twelve- month position; Pay Grade 19, FLSA: Exempt
Experience	A minimum of five years of progressively responsible experience as programmer, analyst, and/or database administrator is required.
Reports to:	Supervisor of Data Systems and Decision Support Services
Supervises:	Data Systems and Decision Support Supervisor
Last Revised	July 14, 2008

Job Description for Senior Systems Analyst
Information Communication and Technology Services

Goal	Coordinates and monitors the development and maintenance of all administrative/business applications of the school division.
Performance Responsibilities	Works closely with users to gather information, clarify system objectives and resolve problems. Provides programming support and technical guidance to the application programmers. Evaluates new systems and applications and presents formal recommendations. Serves as database administrator. Develops and enforces programming and database policies, procedures and standards to ensure integration and maximum performance of systems and applications. Oversees the installation of software patches, fixes and version upgrades and new installations. Prepares and receives Requests for Proposals (RFP). Assists with vendor selection. Assists in the planning and development of the technology budget. Assists in the development and maintenance of a disaster recovery plan. Performs other related duties as assigned.
Education	Bachelors' degree required in Computer Science, Information Systems or related field.
Qualifications	Proficiency in RPG/400 programming required. Experience with SQL and Oracle databases preferred. Programming experience in C++, Visual Basic and SAS desirable. Experience with K-12 education applications highly desirable. Project development and management experience required. Excellent analytical and problem-solving abilities required. Must have the ability to work well with people in all levels of the organization. Must be able to handle multiple projects and requests for assistance in an organized manner with little or no supervision. Must have excellent public relations skills, excellent "customer service" attitude and positive work ethic.
Other Qualifications	Must have a valid Virginia Motor Vehicle operators' license and be able to travel locally to schools and departments.
Pay Scale	Twelve- month position; Pay Grade 19, FLSA: Exempt
Experience	A minimum of five years of progressively responsible experience as programmer, analyst, and/or database administrator is required.
Reports to:	Supervisor of Data Systems and Decision Support Services
Supervises:	Data Systems and Decision Support Supervisor
Last Revised	July 14, 2008

Job Description for System Programmer Analyst
Information Communication and Technology Services

Goal	Develops, writes, maintains, tests, and implements program code as directed and specified through user requests.
Performance Responsibilities	Develops, writes, maintains, tests, and implements program code as directed and specified through user requests. Maintains current knowledge about Student, Human Resources, and Financial Applications Systems supplied by manufacturer or develops in-house. Analyzes user requests to determine appropriate design and implementation methodology consistent with departmental goals and objectives. Designs applications and writes code to develop, maintain, and enhance employee applications as identified by user request. Tests all programs with test data and reviews results for accuracy and efficiency. Tests and implements corrections and releases supplied by the manufacturer in an optimal manner without adverse effect on current production and developmental activities. Troubleshoots and corrects production problems. Updates system and program documentation to reflect changes. Supports student information system and assigned system. Performs other related duties as assigned.
Education	Bachelor's degree in a computer-related field.
Qualifications	Must have a minimum of five years experience in K12 applications systems. Must have extensive knowledge and hands-on experience in RPG/400, RPG III, and RPG ILE. Must have programming experience in CIMS consisting of Student Management, Human Resource Management, and Financial Management. Considerable knowledge of IBM mid-range and microcomputer applications and CIMS software experience required. Must have strong analytical and problem-solving abilities. Experience with student accounting systems in a large urban public school system is preferred. Excellent oral and written communication skills required. Must possess superior customer service, organizational, and planning skills along with excellent communication and public relations skills.
Other Qualifications	Must have the personality and ability to establish and maintain effective working relationships with school staff, employees and other customers. Must possess the ability to work under pressure and effectively plan, organize, and coordinate work independently and/or as a team leader. Must be able to exercise tact, good judgment, and initiative and demonstrate excellent skills in operating personal computers and peripheral equipment. Must be adaptable to changing priorities and able to simultaneously handle multiple assignments within deadlines.
Pay Scale	Twelve-month position; Grade 17, FLSA: Exempt

Job Description for System Programmer Analyst
Information Communication and Technology Services

Experience	Must have a minimum of five years experience in K12 applications systems.
Reports to:	Reports to Senior Systems Analyst
Supervises:	
Last Revised	July 14, 2008

Job Description for Data Administrator
Information Communication and Technology Services

Goal	Gathers, analyzes, and defines user requirements for data access and usability in accordance with division goals.
Performance Responsibilities	Uses query tools, MS Excel, and other business intelligence tools to create reports for schools and division administrators. Identifies and resolves data quality issues such as integrity, accuracy, and completeness in a cost-effective and timely manner. Performs data audits on a regular basis. Identifies causes of data discrepancies and develops procedures to ensure data consistency. Maintains a metadata repository. Develops training materials and conducts user training. Reviews state and federal reports for accuracy and completeness. Contributes to the team effort by accomplishing other related duties that may be required for the effectiveness and efficient operation of the division.
Education	Bachelor's Degree in Computer Science, Information Systems, or any related field is required.
Qualifications	Must have experience with query and business intelligence tools is preferred. Must have strong written and oral communication skills. Must be highly motivated and self directed. Must have analytical skills with keen attention to details. Must have the ability to effectively prioritize and execute tasks in a high-pressure environment. Must be able to establish and maintain professional working relationships with school staff, employees and other customers. Experience with AS/400 and CIMS is helpful.
Other Qualifications	Must be able to work independently with minimum supervision, adaptable to changing priorities, effectively manage and complete multiple assignments within deadlines.
Pay Scale	Twelve-month position; Pay grade 18, FLSA: Exempt
Experience	Minimum of 2 years of experience in the related field required.
Reports to:	Supervisor of Data Systems and Decision Support Services
Supervises:	
Last Revised	July 14, 2008 (previous rev. 8-23-06)

Job Description for Web Support Specialist
Information Communication and Technology Services

Goal	Maintains the school division's intranet by managing links and updating information in pages and databases so that content is kept current.
Performance Responsibilities	Maintains the school division's intranet by managing links and updating information in pages and databases so that content is kept current. Develops, researches, designs, writes, and edits sections and features of the intranet. Consults on Web technology and current and new applications. Assists in planning and development of the technology budget. Troubleshoots intranet/internet problems ranging from programming to hardware configuration. Analyzes intranet traffic statistics and reports relevant information. Performs other related duties as assigned.
Education	Associate degree in Computer Science, Communications, Information Systems or field. Bachelor's degree preferred.
Qualifications	Web development experience required on Windows and Unix platforms. Demonstrated experience with Web technologies such as HTML, XML, JSP and ASP. Demonstrated experience with program forms and implementing scripts using languages such as Java, C++ and Visual Basic. Working knowledge of basic composition, page layout, art and presentation packages such as Front Page, MS Word and Dreamweaver. Experience with security technologies such as PKI, RSA, and Verisign highly desirable. Experience with relational databases such as Oracle and SQL desirable. Proficiency in MS Office. Strong design sense along with a methodical attention to detail.
Other Qualifications	Must have excellent oral and written communication skills and be able to work well with people in all levels of the organization. Must be adaptable and willing to subordinate own image of intranet to that of users and management. Must have the ability to work as a team member and independently with minimal supervision.
Pay Scale	Twelve-month contract position; Pay Grade 17, FLSA: Exempt
Experience	Minimum two years' experience in Web design and development is required.
Reports to:	Supervisor of Data Systems and Decision Support Services
Supervises:	Web Site Design Intern
Last Revised	July 14, 2008 (previous rev. April 9, 2003)

Job Description for Web Site Design Intern
Information Communication and Technology Services

Goal	Assists in the development, implementation, and maintenance of creative, innovative Web page designs for designated sites.
Performance Responsibilities	Assists in the development, implementation and maintenance of creative, innovative Web page designs for designated sites. Helps to develop procedures to ensure that assigned Web site data is factual, current and up to date. Provides assistance in the maintenance of the district's intranet by managing links and updating information in pages and databases to ensure that the content is kept current. Provides assistance in the development, research, design, and edit of sections and features of the intranet as assigned. Performs skilled Web site design and responsible administrative support tasks in an office environment. Accomplishes related work as required.
Education	Minimum high school education. Post secondary education a plus.
Qualifications	Working knowledge of HTML and the use of Macromedia Dreamweaver and FrontPage required. Must have excellent knowledge of communication arts, graphic design, digital imaging, computer graphics and Internet and intranet software applications, procedures and practices. Must have excellent graphic design skills and hands-on experience with Fireworks or Photoshop applications. Excellent oral and written communications, organizational and time management skills are required. Must have excellent creative problem-solving and conceptualization skills.
Other Qualifications	Must have the ability to establish and maintain effective working relationships with others and must be adaptable to changing priorities. .
Pay Scale	Part-time temporary employment, 20-25 hours per week $10.00/Hour, with no benefits
Experience	Minimum of six months of Web site development and design experience. Experience in communication Arts and Design with Windows-based computers and related software required.
Reports to:	Reports to Web Support Specialist
Supervises:	NA
Last Revised	July 14, 2008 (previous rev, 3/11/05)

Job Description for Network Analyst
Information Communication and Technology Services

Goal	Installs and troubleshoots DOS, Windows 3.1, Windows 95, OS/2, Mac OS, and Novell 3.x/4.x systems.
Performance Responsibilities	Setups and maintains the division's WAN as it relates to the internet; connectivity security/logins, software upgrades, and TCP/IP applications. Installs and troubleshoots DOS/WIN, OS/2, Apple/Macintosh and other operating system software on LANS. Assists with the integration of new technologies (i.e., fax/modems, servers, etc.) onto the WAN. Supports wiring, communication and cabling networks including CM' 5, fiber, Ethernet, token-ring, Apple Talk, TCP/IP, CISCO routers & firewalls, 3-COM hubs, twisted pair, ISDN and SMDS. Maintains liaison with vendors of hardware/software cabling and wiring systems used by the division. Maintains schematics and documentation of the district's WAN. Organizes and manages security standards for the LAN/ WAN. Assists in developing and maintaining hardware, software and network standards. Provides help desk support for schools and central administration as needed. Performs other related duties as assigned.
Education	A bachelor's degree in a computer related field and Novell CNE certification preferred. An equivalent combination of education and experience providing the necessary abilities and skills may be substituted.
Qualifications	Must have hands-on experience in configuring and trouble-shooting Novell networks and a working knowledge of CISCO routers, 3-COM hubs, Kalpana switches, CISCO PIX firewalls and other communications hardware/ software is essential. Must have extensive experience in the installation of PC hardware and software including Windows 3.1, Windows 95, Mac OS, Unix, Microsoft Office, Client TCP/IP software including electronic mail, telnet, Web browsers, Netscape, and Eudora mail. Experience with TCP/IP, ISDN and SMDS is important. Setup and maintenance of internet security login Ids, software upgrades, Web browsers and editors and HTML is imperative. Must have proficiency in wiring/cabling topologies including twisted pair coax, category 5, fiber optics, Ethernet and token ring. Must have knowledge of TCP/IP protocols, including LAN and WAN communications, domain name logic and addressing, IP client workstation and server addressing. AS/400 and Windows NT experience helpful.
Other Qualifications	Project management and integration of network design experience is beneficial.
Pay Scale	Pay Grade 17, FLSA Exempt
Experience	A minimum of one years' experience is required.
Reports to:	Reports to Network and Telecommunications Supervisor
Supervises:	Network Analyst Technician
Last Revised	July 14, 2008 (prev rev 05/15/2006)

Job Description for Network Analyst Technician Information Communication and Technology Services

Goal	Performs difficult skilled network analysis and repair, development and maintenance work, and a variety of network support tasks in an office environment; does related work as required.
Performance Responsibilities	Responds to network outages and trouble calls at our 60 Richmond Public Schools buildings throughout the City of Richmond. Works with school staff to assess, diagnose, mitigate, and resolve connectivity issues within the building LAN by reviewing network documentation, observing reported symptoms, and tracing physical connections. During the troubleshooting process must be prepared to temporarily rewire network infrastructure, physically replace bad equipment, and open support calls with specific manufactures and vendors. Installs, configures, documents, maintains, upgrades, and troubleshoots network switches and routers and other network devices. Maintains network documentation including updating Visio network diagrams, logging of network changes, tracking inventory of network equipment and IP addresses. Provides specifications for generation of quotes by vendors on network wiring installation. Maintain communications with wiring and integration vendors to ensure work is completed as designated. Performs other network related duties as assigned.
Education	High School Diploma. Some college preferred
Qualifications	Cisco Certified Network Associate (CCNA) certification or higher required. Certifications in other networking technologies including switching and routing, network security, physical wiring, and network design are preferred. Must possess excellent customer service, organizational and planning skills along with excellent communications and public relations skills. Must have at least two years of experience installing, configuring, maintaining, and troubleshooting Cisco switches, routers, firewalls, and other LAN / WAN equipment. Must have a working knowledge of network diagnostic testers and some experience with Fluke OneTouch is preferred. Must have familiarity with CAT 5E wiring standards and previous network wiring experience. Must have the ability to provide part specifications for generation of quotes for network wiring installation. Must have a working knowledge of Microsoft Visio and the ability to learn other similar applications used for network documentation.

Job Description for Network Analyst Technician Information Communication and Technology Services

Other Qualifications	Must be willing to travel locally with personal vehicle. Must be able to work independently with minimum supervision and effectively manage multiple priorities. Must have the ability to work efficiently under pressure to resolve network outages whenever they occur. Must be available to work after normal work hours and on weekends as required to perform network maintenance. Must be able to communicate efficiently in technical or simple terms as appropriate to end users, staff, and management. Must have the personality and ability to establish and maintain effective working relationships with school staff, employees, and other customers. Must be adaptable to changing priorities and able to simultaneously handle multiple assignments within deadlines. Work is performed under minimum supervision. This is sedentary work requiring the exertion of up to 10 pounds of force occasionally and a negligible amount of force frequently or constantly to move objects. Work requires stooping, kneeling, crouching, reaching, pulling, lifting, fingering, grasping, and repetitive motions. Vocal communication is required for expressing or exchanging ideas by means of the spoken word, and conveying detailed or important instructions to others accurately, loudly, or quickly; hearing is required to perceive information at normal spoken word levels, and to receive detailed information through oral communications and/or to make fine distinctions in sound. Visual acuity is required for preparing and analyzing written or computer data, operation of machines, and determining the accuracy and thoroughness of work; the worker is not subject to adverse environmental conditions.
Pay Scale	Twelve month contract
Experience	Minimum two years related experience is required.
Reports to:	Reports to Network Analyst
Supervises:	NA
Last Revised	July 14, 2008 (previous revision 2/14/08)

Job Description for Records Technician
Information Technology and Communications Services

Goal	Performs storage and retrieval tasks related to student and employee records in a customer-service environment.
Performance Responsibilities	• Pleasantly greets walk-in inquiries from the general public and answers the telephone using the standard four-part greeting effectively handling numerous telephone requests and walk-in customers on a daily basis. • Opens, date stamps and sorts numerous pieces of mail daily and operates a personal computer, copy machine, fax and any other office equipment required. • Plans, initiates and completes office support activities by following up on work in progress and coordinating to ensure timely customer service is provided. • Maintains and works with confidential information on a daily basis. • Performs general clerical work of a varied nature, including moderately complex filing, record keeping, and filling requests for cumulative student records and/or other microfilmed documents. • Verifies attendance and graduation data for employers, probation officers and other authorized parties to include the Division of Motor Vehicles. • Maintains files on current and/or past record requests. • Ensures accuracy of information and abides by the Privacy and Freedom of Information Acts. • Establishes and maintains effective working relationships with personnel in the schools, other offices, governmental agencies and other community agencies. • Maintains supplies as required. • Searches, complies and prepares data for periodic reports on information/reports obtained. • Performs other related duties as required
Education	High school diploma or its equivalency.
Qualifications	• Some experience as a receptionist along with the ability to provide exceptional customer service is required. • Excellent oral and written communication, customer service, public relations and organizational skills are required. • Must have the ability to file and retrieve records in either paper and/or in electronic format. • Must have the ability to work independently under minimum supervision and/or as a member of a team. • Must have the ability to effectively manage and complete multiple deadline actions and to work efficiently under pressure. • The ability to maintain confidential data and information is essential. • Experience is required with window-based computers, Microsoft Word

and Excel applications.

- Some experience with (AS 400) Mainframe access, Internet, Intranet and E-mail applications.
- Must have the ability to effectively work in a cooperative and collaborative manner with coworkers, school staff, students and the general public

Pay Scale

Experience A minimum of one-year experience in the operation of microfilm equipment, cataloging and filing procedures is preferred.

Reports to: Records, Documents, and Publications Services Supervisor

Supervision NA

Last Revised July 29, 2008

Job Description for Telecommunications Technician Information Technology and Communications Services

Goal	Performs all maintenance, installation for voice/data cable plants, telephone equipment, and data network components.
Performance Responsibilities	• Maintains and installs CAT3, CATS and other forms of multi-pair copper cable. • Maintains and installs multi and single mode fiber optics. Installs and maintains all electronic key systems owned by the school division. • Coordinates and supervises contracted telephone work. • Conducts necessary preventative maintenance measures for data hubs, routers, and switches. • Investigates, repairs, and conducts moves and changes from requests submitted by schools and departments. • Maintains and is accountable for school division assigned truck PMS. • Maintains and is accountable for area stocking voice and data components. • Conducts inventory by make, model and serial number of telephone systems and data components twice a year. • Participates in seminars and training focusing on current voice-data technologies. • Provides user training software support to telephone and voice mail systems. • Performs other related duties as assigned.
Education	High school diploma is required.
Qualifications	• Must have proven experience (SMP or Lucent certification) installing and terminating structured cabling, including fiber optics, CAT3, CAT5, and other multi-pair copper. • Must have demonstrated knowledge of methods of providing cabling pathways/proper termination, testing, troubleshooting and labeling schemes for all installations. • Experience and certification in the installation and maintenance of electronic key systems Samsung, Panasonic, Lucent, NEC. Experience with hubs, switches, routers and other network electronics devices, Cisco certification a plus. • PC literacy should include Excel, Word, and PowerPoint. • Excellent organizational skills, ability to work independently and implement effective decision making skills toward completion of assigned tasks. • Ability to communicate both verbally and in writing and work in a cooperative manner with school staff other RPS employees and community and service provider representatives. • **Necessary Special Requirement:** Must possess a valid Virginia motor vehicle operator's license with a good driving record.
Pay Scale	Grade 11 Twelve-month position, **FLSA:** Exempt
Experience	A minimum of four years experience with a reputable telephone company

	or as integrator in the support and installation of voice and data equipment and cable plant.
Reports to:	Network and Communications Services Supervisor
Supervision	NA
Last Revised	July 26, 2008