Metro

Administrative Services Department

Internal Controls Review

December 1998

A Report by Pacific Consulting Group
Issued by the Office of the Auditor

METRO

1998-10136-AUD

Alexis Dow, CPA
Metro Auditor

600 NORTHEAST GRAND AVENUE | PORTLAND, OREGON 97232 2736
TEL 503 797 1891 | FAX 503 797 1831

METRO

OFFICE OF THE AUDITOR

December 10, 1998

To the Metro Council and Executive Officer:

As part of their evaluation of Metro's InfoLink project, Pacific Consulting Group studied Metro's internal controls over the PeopleSoft purchasing and human resource applications as well as its general controls over the InfoLink system.

This report describes the consultants' observations and recommendations regarding these internal controls. Another report issued under separate cover addresses InfoLink project planning and management, system selection and project implementation.

Pacific Consulting Group recommends changes in three areas of internal control:

- Improving controls over changes to computer programs by limiting access to programs
- Developing new procedures and policies to prevent data entry, data validation and other errors and to ensure proper tracking of system users, and
- Enhancing data security by improving passwords and ensuring timely installation of system updates.

Metro staff responsible for implementing and operating the PeopleSoft modules and other systems have worked, and continue to work, diligently and intensely. Pacific Consulting Group's observations suggest that additional resources are necessary to adequately staff continuing implementation efforts and day-to-day operations of InfoLink.

We reviewed this report with the Executive Officer and Chief Financial Officer. The written response of Executive Officer Burton follows the Pacific Consulting Group report.

We appreciate the cooperation and assistance provided by staff in the Administrative Services Department.

Very truly yours,

Alexis Dow, CPA
Metro Auditor

Auditor: Doug U'Ren

METRO AUDITOR

INTERNAL CONTROLS REVIEW OF PEOPLESOFT PURCHASING AND HUMAN RESOURCES APPLICATIONS

FINAL REPORT

DECEMBER 1998

PACIFIC
CONSULTING
GROUP, INC.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

This report presents the results of Pacific Consulting Group, Inc.'s (PCG) review of internal controls over the PeopleSoft Purchasing and Human Resource applications, as well as general controls over the InfoLink system. A separate, higher level review of internal controls over the InfoLink system was performed by Deloitte & Touche LLP, Metro's current external financial auditor.

PCG's review focused on:

- Manual and automated controls restricting access to data on client workstations (or desktops) and the servers.
- Manual and automated controls related to changes in PeopleSoft application program code.
- Manual and automated controls related to protecting the system software, data and network security.
- Application processing controls and segregation of duties within each of the two PeopleSoft applications.

Metro began the implementation of the current Human Resource and Purchasing applications in 1996 with the selection of the PeopleSoft applications software. The Purchasing application was implemented in August 1997, and the Human Resource application was implemented in March 1998. More information regarding the InfoLink system can be found in our related report, "InfoLink Project Review" issued concurrent with this report.

We reviewed documentation, conducted interviews and made observations during our fieldwork for this project. We also reviewed the most recent management letter dated October 24, 1994, from KPMG Peat Marwick, Metro's former financial auditors.

Our evaluation was limited to the two applications – Purchasing and Human Resources. However, during the course of our work, we also evaluated general controls, which are included in this report. Fieldwork was completed between August 10 and September 4, 1998.

We recommended changes in three areas of internal controls:

1. Improving controls over changes to computer programs by limiting access to the programs used to operate the PeopleSoft applications and better controlling employee access to the computer system.

2. Developing controls over processing of the PeopleSoft applications by implementing new procedures and policies for operation of the new system.

3. Enhancing data security policies related to network and UNIX operating system passwords and ensuring updated computer operating system programs are installed in a timely fashion.

Each of these recommended changes is more fully discussed below in Sections II, III, and IV of this report. A summary of our recommendations is provided in Section V.

II. IMPROVING CONTROLS OVER CHANGES IN COMPUTER PROGRAM CODE

Periodic changes to the underlying computer program code for the PeopleSoft software applications are necessary for a number of reasons. Examples include:

- Updating software
- Updating source data
- Fixing problems with program functions
- Correcting errors in source data.

Access to program code should be restricted because it allows an individual to alter both the underlying data and the way in which data is processed by the applications. Changes to programs must be properly documented and supervised to ensure that they are authorized and properly tested prior to implementation. Clearly defined policies and procedures, as well as clear lines of responsibility, guard against unintentional and intentional circumvention of controls.

Access to Computer Program Code

▶ ***Observation:*** Information Management Services (IMS) Division staff is responsible for making necessary changes to PeopleSoft computer program code. Current safeguards are inadequate. Policies and procedures have not been developed to limit capability to change program code. Separate environments for development, testing and production use have not been implemented.

Significance: The potential exists for damaging changes to PeopleSoft program code and the underlying data used by PeopleSoft. This could result in faulty data, IMS producing erroneous reports, as well as intentional circumvention of controls.

Recommendations:

1. We recommend that IMS limit access to program code and give read/write capability to production program directories only to designated system security administrators and their backup staff. This capability should be granted only to staff responsible for UNIX security and local area network (LAN) security.

2. IMS should install separate development, testing and production environments. This will allow full testing of program changes before they are moved into the production environment.

3. Policies and procedures for managing program code changes should be developed and put in place as soon as possible. They should include:
   - Formal review, approval and sign-off of any PeopleSoft program code changes by user management before the changes are moved from the test to the production environment.
   - Clearly defined roles and responsibilities for all members of the InfoLink project team and the IMS system administrator.
4. Metro should evaluate commercially available software "librarian" packages for managing program source code on the Hewlett-Packard server.

PeopleSoft Access – Superusers

▶ ***Observation:*** Metro currently has 13 individuals with superuser access to the PeopleSoft financial applications (e.g., Purchasing and Accounts Payable) and six individuals with superuser access to the Human Resource applications.

Significance: Superuser access allows individuals unlimited access to all functions within the PeopleSoft applications, including the ability to give access to other users for capabilities that they were not intended to have. Full access to all functions allows users to circumvent controls. For example, a superuser could both enter and approve payment for an invoice or change underlying system data such as employee pay rates.

Recommendations:

1. Reduce the number of Metro staff with superuser access to the security administrator for the Hewlett-Packard and LAN server, the database administrator and the system administrator.
2. Make access to PeopleSoft applications consistent with each individual's job responsibilities. Full access to all functions in the production system is not consistent with any one individual's job, except for those listed in the previous recommendation.
3. Develop written policies and procedures for granting superuser access rights in the system. The Administrative Services Department director should authorize all superusers in writing and should be excluded from superuser access.

PeopleSoft Access – Passwords

▶ ***Observation:*** The PeopleSoft applications do not require users to change their passwords on a 60-day basis as is required for the Novell network. It is common for a single password to be used by multiple staff and outside consultants working on projects like InfoLink during development. We were unable to confirm that passwords were changed when the InfoLink system moved from development to production.

Significance: It is important to ensure that proper controls to limit access to the system are implemented. This helps ensure that only authorized individuals have access to the system and that they perform functions related only to their job responsibilities. Inappropriate access allows users to intentionally or unintentionally alter program code and data.

Recommendation: Prior to implementing version 6.0 of the PeopleSoft financial applications, all user identifications and passwords should be revoked and replaced. This will ensure that appropriate levels of system access are established.

Security Classes

- ***Observation:*** Metro currently has 21 active security classes for the PeopleSoft financial applications and 10 active security classes for the Human Resource applications. Security classes define groups of individuals with the same access to screens within PeopleSoft applications. They provide capabilities to update and display, add and correct data shown in PeopleSoft.

  Significance: The high number of security classes increases the effort required to monitor and maintain the classes, although it does not indicate a control weakness.

  Recommendation: Metro should review the number of classes to determine if they can be reduced as part of the version 6.0 implementation.

III. Developing Controls Over Processing in PeopleSoft Applications

Clearly defined responsibilities and segregation of duties are needed during the transition to a new computer system to prevent the data entry, data validation and other errors that often occur. Written policies and procedures are especially useful with a small number of staff, where few individuals are familiar with day-to-day operations of the system. Formal procedures also help ensure proper tracking of those added and deleted as system users and of authorization of their access.

Policies and Procedures – Clear Definition of Responsibilities

▶ ***Observation:*** Written policies and procedures for the uses of the Human Resources and Purchasing applications have not been developed. Metro also lacks formal documentation describing the specific duties of user departments, Purchasing, and Human Resources staff for entering, reviewing and correcting information in the system.

Significance: Since much of the knowledge is vested in a limited number of Metro individuals, staff attrition can adversely affect system operations. The lack of clearly defined responsibilities during system implementation has resulted in errors at other clients, although we did not observe specific processing errors at Metro. While work has been initiated in some areas, such as Human Resources and Accounts Payable, formal procedures should be completed for all PeopleSoft applications. The lack of formal policies and procedures increases the time, cost, and risk of error in training new employees or assigning staff to temporarily work in another area.

Recommendation: Metro should facilitate the InfoLink implementation by defining organizational responsibilities for the PeopleSoft applications and making certain that users are trained and understand their roles. Written control procedures should be developed to ensure that:

- Appropriate personnel review output reports for completeness and accuracy
- Output reports are balanced routinely to relevant control totals
- Errors are corrected and resubmitted
- Day-to-day system operations are adequately documented.

Policies and Procedures – Tracking System Access

▶ ***Observation:*** Formal procedures have not been adequately documented to ensure those terminating employees or employees transferring to new job responsibilities

within Metro are denied access to the PeopleSoft system. Informal procedures have not been routinely followed to ensure the prompt removal or modification of Metro employees' system access due to termination or transfer. Outside contractors' system access has not been removed in a timely manner following contract completion.

Human Resources staff currently uses an e-mail distribution list to notify various Metro staff of an employee's resignation or termination. The e-mail is intended to inform IMS staff when to revoke system access for the separating employee.

Significance: Employees who have terminated from Metro should not be given access to Metro information systems. Continued access is inappropriate. Depending on the level of access, former employees could make inadvertent or intentional changes to data or program code, as well as obtain information to which they should no longer have access. The access level of employees who have transferred to different jobs within Metro needs to be evaluated to ensure it remains appropriate.

Recommendation: Human Resources staff should develop formal procedures to supplement the current e-mail distribution list. These procedures should include positive, written documentation to ensure that employee network and application access is revoked before or at employee separation or modified when an employee transfers to a new position. Outside contractor access to the system should be revoked upon contract completion. A checklist, maintained by Human Resources, verifying that system access has been revoked by IMS, would assist in this process.

Processing Controls – Access and Segregation of Duties

- ***Observation:*** There appear to be two Metro employees with inappropriate access to Purchasing and Accounts Payable applications.

  Significance: Inappropriate access and inadequate segregation of duties allow inadvertent or intentional misuse of the system. It is important to separate the ability to add vendors from the ability to pay them within the financial system.

  Recommendation: Access to Purchasing applications should be reviewed to ensure that access rights granted to individuals within security classes CLSS5GLP and CLASS5PO remain appropriate. The ability to add vendors should be restricted to Purchasing staff. The implementation of PeopleSoft version 6.0 will require reestablishing all system security accesses. Metro should review system access for all classes of users at that time to ensure that there is appropriate separation of duties.

Processing Controls – Authorization for Access

- ***Observation:*** Access to the PeopleSoft financial applications was granted without written authorization. In most cases, it was granted when the InfoLink system was first implemented. Although written authorizations were maintained for access to the

Human Resource applications, Metro has not developed formal policies and procedures for access to the system.

Significance: The lack of proper authorization can result in inappropriate access to PeopleSoft applications, which can result in unintentional or intentional alteration of data stored in the system.

Recommendation: IMS should continue efforts to develop procedures for authorizing and documenting access to PeopleSoft applications.

IV. ENHANCING DATA SECURITY

Security measures prevent unauthorized access to the system by those who may inadvertently or intentionally make changes to computer programs or data. They help ensure users have system access that matches their qualifications, training and job responsibilities.

Hewlett-Packard periodically issues security patches for the network server to correct identified problems or errors in the UNIX operating system. The patches normally identify the type of problem to be corrected and any prior patches that also must be installed. It is important to maintain a relatively current operating system to prevent known problems from occurring in Metro's computing environment.

Network Passwords

- ***Observation:*** Metro's Novell network servers require employees to change their passwords every 60 days. The system checks new passwords to ensure that they have not been used for at least eight consecutive times by their respective users. There are no restrictions on current passwords, which may include any combination of letters, numbers or special characters. Exhibit IV-1 provides examples of common, easily broken passwords.

  Significance: Metro's policies do not require the use of a secure password configuration. The current password configuration may be easily broken using available software programs. There is a significant opportunity for unauthorized access to Metro's information systems because the network has access to external networks. As additional access to Metro's network is provided via the Internet, facsimile machines on the network, and dial-up modems, more secure access procedures should be implemented.

  Recommendation: Metro should evaluate requiring employees to create passwords that are more complex to prevent employees from selecting passwords that can be easily broken.

Exhibit IV-1
Examples of Easily Deciphered Passwords

Password	Logic Problem
alec7	It is based on a user name
tteffum	It is based on a user name
gillian	Name is in a dictionary
naillig	Name is in a dictionary (backwards)
PORSCHE911	It is in a dictionary
12345678	It is in a dictionary and is easy to type
qwertyui	It is in a dictionary and is easy to type
abcxyz	It is in a dictionary and is easy to type
Ooooooo	It is in a dictionary and is easy to type
Computer	It is in a dictionary and is easy to type
wombat6	It is in a dictionary and is easy to type even with a random character
6wombat	It is in a dictionary and is easy to type even with a random character
merde3	Common French word with added character
zeolite	It is in a geological dictionary
ze01lte	It is in a geological dictionary
mr.spock	It is in a science fiction dictionary

Network Server Security

- ***Observation:*** We were unable to determine who has the root password to the Hewlett-Packard server or verify that all security patches for the server have been installed.

  Significance: Inappropriate access to computer programs or data on Metro's UNIX server can result in significant problems in Metro's computing environment. Within the UNIX operating system on the server, the "root" is where all log and configuration files are kept. The root password allows access to all programs and data on the server. Failure to install security patches can also cause network problems.

  Recommendation: The Chief Financial Officer should develop formal policies and procedures for root password access. The root password should be limited to a very select group of individuals required to maintain the system. The IMS Division Manager should maintain written authorization of individuals with root password access and review the following items on a quarterly basis:

  - The list of individuals having the root password for the server. Access should be limited to only those system and UNIX administrators within IMS who operate the server.
  - The installation status of all security patches issued by Hewlett-Packard for the server operating system.
  - Maintenance or changes to the root password.

V. SUMMARY OF RECOMMENDATIONS

The following is a list summarizing our recommendations to improve internal controls over the PeopleSoft Purchasing and Human Resource applications as well as general system controls.

- Limit access to production computer programs of the PeopleSoft modules to the UNIX and local-area-network (LAN) security administrators.

- Implement separate computing environments for production, test, and development for use with the PeopleSoft modules.

- Develop and implement formal policies and procedures for managing program changes.

- Evaluate the purchase of commercial “librarian” software to manage the movement of programs from development, test, and production.

- Reduce the number of staff with ”superuser” access to the PeopleSoft modules to the administrators for Hewlett-Packard and LAN security, the database, and the PeopleSoft system.

- Develop and implement written policies and procedures for system access.

- Update user identification and password codes in conjunction with the implementation of the PeopleSoft 6.0 upgrade.

- Reduce the number of security classes for the financial and human resource applications in conjunction with the PeopleSoft 6.0 upgrade.

- Define organizational responsibilities for use of PeopleSoft applications and train users in the various roles and responsibilities associated with the system.

- Develop written procedures for reviewing and verifying system reports, correcting errors, and operating the PeopleSoft applications.

- Develop formal procedures to ensure that employee network and application access is revoked before or at employee separation.

- Review access rights to the Purchasing application to ensure that the rights granted to individuals remain appropriate.

- Require employees to create more complex passwords for access to PeopleSoft applications.

- Develop formal policies and procedures for UNIX root password access.

The above internal control recommendations should not only be implemented for the Purchasing and Human Resource applications, but should also be considered for relevance in other existing and future applications at Metro.

Response to the Report

M E M O R A N D U M

METRO

Date: December 8, 1998

To: Alexis Dow, Metro Auditor

From: Mike Burton, Executive Officer

Re: **Response to Internal Controls Review**

Thank you for the opportunity to review and comment on the audit by Pacific Consulting Group on Internal Controls. We appreciate the professional review of Metro's internal controls on access to PeopleSoft applications.

It is significant to note that Metro has been in a continuous implementation mode for over two years, with financial and human resources modules that have stretched the available resources in both technical and functional areas.

Three important points must be taken into account regarding security:

1. PeopleSoft security is complex and time consuming. PeopleSoft, in its initial RFP response, did not suggest adding resources for this function. Metro expected to use a similar level of resources to those used in the old mainframe environment. To implement the controls and documentation recommended in the audit will require significant resources, perhaps as much as one full-time employee.

2. PeopleSoft has two "levels" of security: basic security and operator preferences. Even if an employee has access to a panel, they may not perform any changes if they do not have the correct operator preference.

3. Version 6.0 has completely different security than version 5.1. Management will review security demands as version 6.0 is implemented. It should be noted that IMS, as the result of an earlier Deloitte and Touche audit, has already committed to develop more comprehensive security policies for all IT systems. The implementation of version 6.0 is a critical part of this.

Regarding the *Internal Controls Review* recommendations:

1. Limit access to production computer programs or the PeopleSoft code to the Unix and LAN security administrators.

Agreement with Recommendation: While we agree in principle, we are concerned that providing only staff responsible for Unix and network security with read/write access to production program directories could create a bottleneck in making changes to the system in emergency situations. We plan to use "split" passwords in which pairs of individuals, other than1he Unix and network security administrators, hold half of a single password to the system.
Proposed Action Plan: Staff will review program code security and options available in conjunction with a general update of IMS' Computer User's handbook.

Proposed Timetable: We propose completing this by the end of the third quarter of third quarter of 1999.

2. Implement separate developing, testing, and production environments.

Agreement with Recommendation: Staff has already created separate databases for development, testing and production that have been used throughout the implementation and production use of financials and HR/Payroll. Furthermore, all software modified by Metro is isolated in directories separate from those for standard PeopleSoft software. Settings in the Windows configuration manager are used to point PeopleSoft to the modified programs. We agree that this separation must be extended to encompass the software development lifecycle.

Proposed Action Plan: Staff will continue to maintain and utilize separate database environments for development, testing and production. A separate environment for source programs will be implemented on a dedicated file server.

Proposed Timetable: Financials: completion by end of the second quarter of 199 (an element of the Financials version 6.0 Upgrade). HR/Payroll: completion by end of the fourth quarter of 1999 (an element of the HRMS version 7.5 upgrade)

3. Develop and implement formal policies and procedures for managing program changes.

Agreement with Recommendation: Our past experience shows that formal policies and procedures for program code management can be extremely cumbersome and labor intensive if not sensitive to the size and workload of the organization. Clearly defined roles are in place for members of the project team, but with limited staff, roles are often shared to assure critical tasks are completed.

Proposed Action Plan: Staff will review formal code management policies and revise as needed in conjunction with a general update of IMS' Computer User's Handbook that will begin in the first quarter of 1999.

Proposed Timetable: We propose completing this by the end of the third quarter of 1999.

4. Evaluate the purchase of commercial "librarian" software to manage the movement of program from development, test and production.

Agreement with Recommendation: Agreed. However, we feel this would add unneeded complexity and costs to an already understaffed environment. This recommendation will be given further consideration when the IMS division is fully staffed.

Proposed Action Plan: Staff will review given budget and time.

Proposed Timetable: Complete review when fully staffed.

5. Reduce the number of staff with "superuser" access to the PeopleSoft modules to the security administrators for HP and LAN, the database administrator and the system administrator.

Agreement with Recommendation: We agree with the recommendation. However, as discussed earlier in this response, this scheme must be augmented with split passwords so that single person reliance is avoided.

Proposed Action Plan: No action is needed.

Proposed Timetable: Not applicable.

6. Make access to PeopleSoft applications consistent with each individual's job responsibilities.

Agreement with Recommendation: We have striven to tailor access to job requirements throughout the implementation. We agree with this recommendation.

Proposed Action Plan: Staff will review the appropriate level of access when version 6 is implemented.

Proposed Timetable: Complete version 6 review by end of the first quarter of 1999.

7. Develop written policies and procedures for granting superuser access rights in the system. The ASD director should authorize all superusers in writing and should be excluded from superuser access.

Agreement with Recommendation: Agreed

Proposed Action Plan: The Director of Administrative Services will prepare policies consistent with practice and fiduciary responsibilities. The ASD Director will not have superuser access.

Proposed Timetable: Complete by end of the first quarter of 1999.

8. Prior to implementing version 6, all user identifications and passwords should be revoked and replaced.

Agreement with Recommendation: As a practical matter, version 6 requires a complete re-implementation because security will not convert from version 5.1.

Proposed Action Plan: Performed with implementation of version 6.

Proposed Timetable: Complete by end of1he second quarter of 1999.

9. Reduce the number of classes of security.

Agreement with Recommendation: Security classes were installed to assure that staff had access to only what they needed to perform job duties as recommended under #6. We agree to reduce security classes where possible.

Proposed Action Plan: Staff will review the number of classes needed as version 6 is implemented.

Proposed Timetable: Complete by end of the first quarter of 1999.

10. Defining organizational responsibilities for use of PeopleSoft applications and train users in the various roles and responsibilities associated with the system.

Agreement with Recommendation: Agreed. Most of the effort on written policies, procedures, and training has focused on central service staff responsibilities. This work needs to be completed and department users need to be included.

Proposed Action Plan: Staff will review and complete written policies and procedures for all PeopleSoft modules. These will serve as a basis for ongoing training for both central service and departmental users.

Proposed Timetable: Complete by end of the second quarter of 1999.

11. Develop formal procedures to ensure that employee network and application access is revoked before or at employee separation.

Agreement with Recommendation: Agreed

Proposed Action Plan: HR will develop, in consultation with IMS, formal procedures to notify PeopleSoft and network security administrators of employees who have:

- transferred and require security to be reestablished, or
- terminated and require security to be revoked.

Proposed Timetable: Complete by end of the first quarter of 1999.

12. Access to purchasing applications should be reviewed and restricted to assure segregation of duties.

Agreement with Recommendation: Agreed. We believe current access properly segregates duties, but we will review system access for all classes of users.

Proposed Action Plan: Security classes will be reviewed as part of the security review during the version 6 Implementation.

Proposed Timetable: Security class review will be completed by end of the first quarter of 1999. User security for Purchasing will be re-established by end of the second quarter of 1999.

13. IMS should continue efforts to develop procedures for authorizing and documenting access to PeopleSoft Applications.

Agreement with Recommendation: Agreed. Note that current security levels and access to PeopleSoft is based on security granted by written authorization under the old mainframe system.

Proposed Action Plan: Security will be thoroughly reviewed as part of the version 6 implementation.

Proposed Timetable: Complete by end of the first quarter of 1999.

14. Require employees to create complex passwords.

Agreement with Recommendation: Agreed. However, because users create their own network passwords and passwords are secret and cannot be monitored it is difficult to enforce this recommendation.

Proposed Action Plan: Staff will determine if Novell has the capability to analyze passwords for complexity or look them up in a dictionary. If available this will be implemented. If not available, staff will undertake an informational campaign to raise awareness of the requirement for creating secure passwords.

Proposed Timetable: Complete by end of the first quarter of 1999.

15. The CFO should develop formal policies and procedures for root password access with written authorization and quarterly review.

Agreement with Recommendation: Agreed.

Proposed Action Plan: The Director of Administrative Services (also serving as the CFO) will prepare policies consistent with practice and fiduciary responsibilities.

Proposed Timetable: Complete by end of the first quarter of 1999.