



Michigan
Office of the Auditor General
REPORT SUMMARY

Performance Audit
Human Resources Management Network
(HRMN) Self-Service
Department of Civil Service (DCS)

Report Number:
19-596-03

Released:
July 2004

HRMN Self-Service is the State's Web-based automated system used by State employees and human resource managers to view and maintain personnel information related to employee benefits, leave balances, pay warrant information and withholdings, and life events. HRMN Self-Service also enables human resource managers to track and maintain human resource reports.

Audit Objective:

To assess the effectiveness of security over HRMN Self-Service.

Audit Conclusion:

DCS did not completely establish effective security over HRMN Self-Service.

Material Conditions:

DCS did not sufficiently evaluate and minimize the risk of providing confidential State employee and dependent data over the Internet through HRMN Self-Service. Appropriate evaluation and risk assessment would minimize vulnerabilities to the State and to State employees resulting from unauthorized access. (Finding 1)

DCS did not completely establish effective access and password controls over HRMN Self-Service. Effective access and password controls minimize the possibility of unauthorized users obtaining access to HRMN Self-Service data. (Finding 2)

DCS had not developed and implemented sufficient Web application security controls. Without the implementation of sufficient Web application security controls, personnel data and Web application resources are vulnerable to intrusion or misuse. (Finding 3)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:

To assess the effectiveness of general controls over HRMN Self-Service.

Audit Conclusion:

The Department of Information Technology's (DIT's) general controls over HRMN Self-Service were reasonably effective.

Reportable Conditions:

DIT had not established controls over the operating system configuration. The operating system should be installed with a minimal service configuration to reduce the risk of intrusion and the exploitation of well-known operating system vulnerabilities. (Finding 4)

DIT had not established complete operating system access controls. This could result in unauthorized modification, loss, or disclosure of confidential State employee data. (Finding 5)

DIT had not established complete physical security controls over HRMN Self-Service resources. Physical security controls help ensure that valuable system resources are safeguarded and that access is limited to individuals responsible for managing the system. (Finding 6)

DIT should strengthen controls over program changes to HRMN Self-Service. Program change controls help ensure that only authorized, tested, and approved program modifications are implemented and that access to and distribution of programs are carefully controlled. (Finding 7)

~ ~ ~ ~ ~

Agency Response:

Our audit report contains 7 findings and 7 corresponding recommendations. The agency preliminary response indicated that DCS and DIT agreed with the 3 recommendations and 4 findings, respectively, pertaining to their operations.

~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: <http://audgen.michigan.gov>



Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General