

OFFICE OF THE CITY AUDITOR

City and County of Honolulu
State of Hawai'i

Audit of the City's Information Security and Risk Management Program



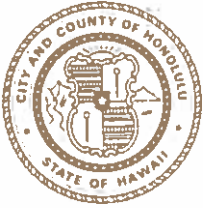
Audit of the City's Information Security and Risk Management Program

A Report to the
Mayor
and the
City Council
of Honolulu

Submitted by

THE CITY AUDITOR
CITY AND COUNTY
OF HONOLULU
STATE OF HAWAII

Report No. 16-04
May 2016



OFFICE OF THE CITY AUDITOR
CITY AND COUNTY OF HONOLULU
1001 KAMOKILA BOULEVARD, SUITE 216, KAPOLEI, HAWAII 96707 / PHONE: (808) 768-3134 / FAX: (808) 768-3135

EDWIN S.W. YOUNG
CITY AUDITOR

May 27, 2016

The Honorable Ernest Y. Martin, Chair
and Members
Honolulu City Council
530 South King Street, Room 202
Honolulu, Hawaii 96813

Dear Chair Martin and Councilmembers:

Our office has completed work on the *Audit of the City's Information Security and Risk Management Program*. This audit was self-initiated by the Office of the City Auditor pursuant to Section 3-502.1(c) of the Revised Charter of Honolulu and the City Auditor's Annual Work Plan for FY2014-15. The audit objectives were to: (1) assess the state and effectiveness of the city's information technology (IT) security management program; (2) assess the implementation of effective user security awareness and security related personnel policies to support IT security; and (3) assess the capability and effectiveness of the city's cybersecurity operations.

Background

Information has evolved into a key asset for the city and requires protection from unauthorized users. The city's increasing reliance on information technology to support government services requires the city's IT security programs to be effective. Security policies and procedures must meet operational and security objectives, and cybersecurity operations should remediate IT security weaknesses. User security awareness and IT-security related personnel policies must support IT security; and responses to IT security incidents must be effective to protect city data, processes, and systems.

Audit Results

Prior audits, consultant reports, and external financial information system audits of city security controls have itemized deficiencies and made recommendations for improving city IT security. Although the new Department of Information Technology (DIT) director has introduced several new technical initiatives to improve and protect the city systems, more needs to be done to ensure the city is not vulnerable to unauthorized access to its data assets, and established controls properly address potential threats.

More specifically, DIT needs to conduct risk assessments that identify and prioritize data assets that should be protected; implement controls that protect the prioritized assets from potential threats; and update security control policies and procedures. DIT needs to provide security awareness training; and test incident response plans.

The Honorable Ernest Y. Martin, Chair
and Members
May 27, 2016
Page 2 of 2

In addition, DIT security information staff need authorization to implement security measures commensurate with their responsibilities; follow up on identified threats; improve communications within DIT and among city departments; and assess and validate security risks.

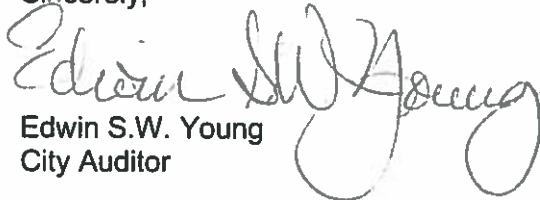
These improvements are needed to ensure unauthorized hackers and system breaches do not occur and, if a breach occurs, the city costs are minimized.

Management Response

The Managing Director and the Department of Information Technology director agreed with 11 of the recommendations and implemented most of the recommendations in response to the draft reports. Due to lack of funding, management did not agree to create an executive position for cybersecurity (see Recommendation #12). The management comments were responsive to the audit recommendations.

A copy of our final draft report is attached. We express our appreciation for the cooperation and assistance provided us by the staffs of the Office of the Managing Director, the Department of Information Technology, and the many other departmental staff and managers contacted during this audit. We are available to meet with you and your staff to discuss the review results and to provide more information. If you have any questions regarding the audit report, please call the auditor-in-charge, Wayne Kawamura, or me at 768-3134.

Sincerely,



Edwin S.W. Young
City Auditor

- c: Kirk Caldwell, Mayor
Roy Amemiya, Jr., Managing Director
Nelson Koyanagi, Jr., Director, Department of Budget and Fiscal Services
Mark Wong, Director and CIO, Department of Information Technology
Keith Ho, Deputy Director, Department of Information Technology
Brian Miyata, Security Administrator, Department of Information Technology

Table of Contents

Chapter 1 Introduction and Background

Introduction	1
Background.....	1

Chapter 2 City’s Network Security May Be Vulnerable to Cyber Attacks

Background.....	7
Audit and Consultant Issues Need to Be Resolved	12
Security Management Oversight Can Be Improved.....	13
Other Security Related Tasks Need to Be Addressed.....	17
Better City Security Coordination Over Its Policy Framework is Needed	28
Recommendations	31

Chapter 3 DIT Security Staff Needs Authority to Implement Security Measures

Background.....	33
Information Security Staff Lack the Authority to Implement Security Measures	34
Remediation of Security Weaknesses Is Needed.....	41
A Chief Information Security Officer Is Needed.....	46
Recommendations	48

Chapter 4 Conclusions and Recommendations

Recommendations	49
Management Response	51

Appendices

Appendix A	Audit Objectives, Scope and Methodology	57
Appendix B	Glossary of Terms and Definitions	59
Appendix C	Risk Assessment	61
Appendix D	Future PCI Assessment Considerations.....	63
Appendix E	Presidio Risk Assessment and Recommendations for Top Ten Critical Findings – City and County of Honolulu (2009).....	65
Appendix F	Critical Security Controls.....	67
Appendix G	Critical Elements for Security Management.....	71
Appendix H	Survey Questions and Results From Departments Regarding Information Technology Systems and Security Policies.....	73
Appendix I	Technology Roadmap	75

List of Exhibits

Contents

Exhibit 1.1 Department of Information Technology (DIT) Organizational Chart3
Exhibit 1.2 Technical Support Division Organizational Chart4
Exhibit 2.1 Office of the City Auditor, Information Technology Systems and Security Policies
Survey Results29
Exhibit 2.2 State of Current IT Plans and Policies30

Chapter 1

Introduction and Background

Introduction

This audit was self-initiated by the Office of the City Auditor pursuant to Section 3-502.1(c) of the Revised Charter of Honolulu and the City Auditor's Annual Work Plan for FY2014-15. The office of the city auditor determined this audit was warranted based on the city's increasing reliance on information technology (IT) based data, processes, and systems to support current government services. The audit objectives were to (1) assess the state and effectiveness of the city's information technology security management program; (2) assess the implementation of effective user security awareness and IT-security related policies and procedures to support IT security; and (3) assess the capability and effectiveness of the city's cybersecurity operations.

Background

Information has evolved into a key asset that has value to many stakeholders and requires protection from unauthorized users. Information technology security controls should preserve the confidentiality, integrity and availability of key information systems, programs, and data. The security management program should therefore establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. In addition, overall city policies, plans, and procedures should be developed and implemented citywide.



In recent years, major enterprises like Target, Home Depot and Sony Pictures Entertainment (Sony) experienced information system breaches that required the companies to pay millions of dollars to cover the costs related to the attacks. In the cases of Home Depot and Target, the intrusion initially occurred via hacked third-party vendors and financial gain was the motivation. For Sony, the company was the apparent victim of an extremely sophisticated malware attack to steal confidential information.

JP Morgan Chase and other financial institutions were also severely affected by data breaches. AT&T reportedly paid \$25 million to settle a data breach that involved the disclosure of personal information of 280,000 U.S. customers. Recently, the Hollywood Presbyterian Hospital in Glendale, California

information systems were infected with *ransomware* malware that threatened to destroy medical records if a ransom was not paid. A recent survey by the Ponemon Institute reported the average cost of cybercrimes for US retail stores more than doubled from 2013 to an annual average of \$8.6 million per company in 2014.

Not only are the attacks more damaging, there also are more of them. PricewaterhouseCoopers reported in its *Global State of Information Security Survey 2015* that the number of detected information security incidents had risen 66 percent since 2009. The 2014 survey further reported that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013. As the breaches became more significant, they also had a significant financial impact.

Governmental entities were also severely affected by data breaches. Typically government entities experience only a disruption of service in the current cybersecurity climate. However, the recent breach of the U.S. Office of Personnel Management affected 21.5 million government workers, and the identity theft costs for the federal government are estimated at \$133.3 million to \$329.8 million. The U.S. Department of Defense has been the victim of attacks and data breaches in its information systems. The General Services Administration awarded \$500 million in purchase agreements for identity monitoring, data breach response, and protection services to mitigate potential damage to those affected. Locally, the Hawai'i state and the 30-Meter Telescope websites were attacked by Anonymous, a hacktivist group, allegedly in protest of the telescope under construction atop Hawai'i's Mauna Kea summit.

Department of Information Technology (DIT) roles and responsibilities

The Department of Information Technology manages most of the city's information technology resources, and is responsible for setting and enforcing citywide technology and data security standards and policies.¹ The department manages the city's computer systems and telecommunications network twenty-four hours a day, seven days a week. To enable DIT to fulfill its

¹ The department manages most of the city's information technology resources. There are some agencies, such as the Board of Water Supply, Honolulu Police Department, Department of the Prosecuting Attorney, Department of Budget and Fiscal Services, Department of Planning and Permitting, and City Council, which either DIT does not support or provides limited support and management of their information technology systems and resources.

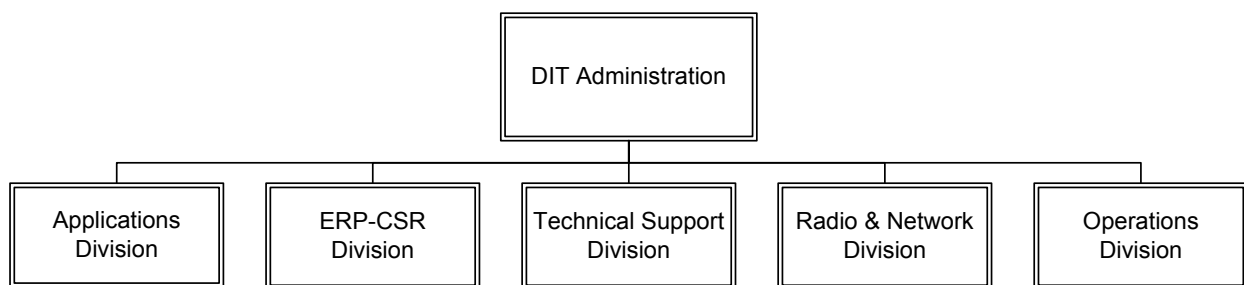
cybersecurity mission, it uses an adaptive security² approach that performs unobtrusively, minimizes the propagation of attacks, and allows for a quick response to known and unknown attacks.

DIT's mission includes developing and directing the integrated system of computer resources that provides data processing and telecommunications services to most city agencies and authorized users. The department is tasked with the centralized management of information technology services to allow users of the city's network to share data, information, technology, resources, and technical expertise in a cost-effective and efficient manner.

DIT is also expected to deliver reliable, efficient, and effective information technology services to city agencies, businesses, residents, and visitors of Honolulu. The department's other roles include advising the Mayor and other departments on the use of technology that automate processes, reduce operating costs, and make government more transparent, responsive, and accountable.

As of FY 2015, the DIT operating budget was \$21.9 million and authorized staffing was 144 full-time equivalents. The department has five operational divisions: Applications, Technical Support, Radio and Network, Enterprise Resource Planning - Computer Service Representative (ERP-CSR), and Operations.

Exhibit 1.1 Department of Information Technology (DIT) Organizational Chart

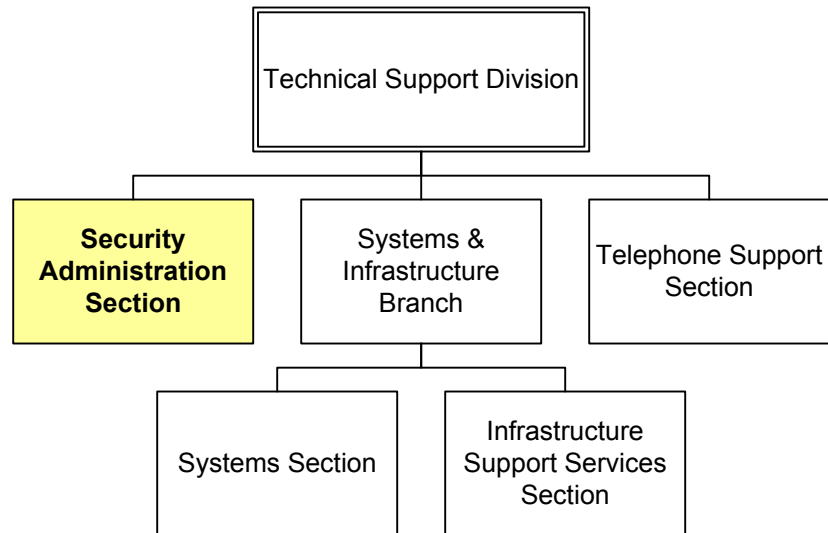


Source: Department and Agency Reports of the City and Council of Honolulu, FY 2015

² Adaptive security is an approach to implement an agile and flexible IT security to deal with the constant change in technology and potential breach, despite whatever technical security solutions are applied. It typically applies tools and techniques to automatically respond and minimize the effects of security incidents.

The Technical Support Division is responsible for protection, security, and integrity of the city’s information resources; enforcing security related policies and procedures; and monitoring and preventing attacks on the city’s information systems. Operating expenditures for the Technical Support Division was \$1.5 million in FY 2015 and staffing totaled 22 full-time equivalents. Its security administration section currently has 4 full-time staff.

Exhibit 1.2
Technical Support Division Organizational Chart



Source: Office of the City Auditor

DIT initiatives

To protect the city’s information system assets and counter potential threats, the director of the Department of Information Technology (DIT) introduced and implemented several initiatives to improve the city’s IT security during his recent tenure. The technical initiatives included:

- Automated scanning for unauthorized devices and applications;
- Continuous malware defenses;
- Extensive data recovery capability;
- Implemented a single sign-on (SSO) across platforms using MIT Kerberos 5 (DIT);

- Implemented public key infrastructure and SSL on major web servers;
- Consolidated various directory services into a single LDAP domain under the control of an Active Directory;
- Introduced continuous synchronization and reconciliation between user accounts and employee transitions in the human resources system (ADsync);
- Integrated identity management for financial systems;
- Recently revamped and adopted a new IT Policy (2015) for the city; and
- Developed lifecycle management of wired and wireless access, networks, and end-user connectivity. See Appendix B for *Glossary of Terms and Definitions*.

There have been no recent major disruptions of IT services due to security-related incidents. The most recent are from the early 2000s, where the city's electronic mail system had to be shut down for a day due to the *ILOVEYOU* virus, and in a separate incident for a few hours due to the propagation of the homepage worm. The department has worked diligently since then to improve its technical security posture to increase its ability to avoid major IT service outages due to security incidents.

This page intentionally left blank.

Chapter 2

City's Network Security May Be Vulnerable to Cyber Attacks

Despite implementing many of the recommendations identified in prior audits, consultant reports, and financial information system audits, more needs to be done to resolve the audit and consultant issues. These include performing risk assessments, prioritizing data assets, and identifying proper controls to protect the city from potential threats. Other security-related tasks, such as security awareness training, and follow up on identified threats are needed to ensure former employees, contractors, and non-users do not gain unauthorized access to city systems. Contingency plans need to be tested and exercised before a breach occurs, security policies and procedures updated, and security communications and actions better coordinated. Strengthening these areas of the city's current IT security program would improve the city's overall security posture.

Background

The U.S. General Accountability Office (GAO) issued several reports on federal information security. In these reports, GAO report that agencies need to correct weaknesses and to fully implement security management programs. The GAO reports also discuss the National Institute of Standards and Technology (NIST) framework for improving critical cybersecurity infrastructure.¹ In these reports, GAO reports:

- The widespread use of the internet and the emergence of increasingly sophisticated cyber threats underscore the need to manage and bolster federal information systems security.
- Cybersecurity deficiencies and weaknesses place federal information and information systems at risk.

¹ GAO-15-714, *Federal Information Security – Agencies Need to Correct Weaknesses and Fully Implement Security Programs* (September 2015) and GAO-16-152, *Critical Infrastructure Protection – Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework* (December 2015).

- The number of information security incidents increased from 5,503 in FY 2006 to 67,168 in FY2014 and identified 6 cybersecurity threats, 10 cyber exploits, and 7 cyber events².
- Discussed weaknesses in access controls, configuration management, incompatible segregation of duties, continuity of operations, information security, and actions recommended to strengthen information security.

Current security management standards and practices recognize that information security involves more than technical tools. They point out that good system security involves five internal controls elements (control environment, risk assessment, control activities, information and communications, and monitoring). An entity should:

- (1) create an inventory of applications, data, platforms, and networks;
- (2) identify and prioritize the resources (e.g. confidential and private data) that should be protected; and
- (3) consider potential threats and the controls needed to mitigate the threats.

It is also recommended that the IT management entities, like the city, should:

- (4) assess risks and the impact of the risks;
- (5) evaluate the operating effectiveness of the controls;
- (6) test automatic and manual, general controls; and
- (7) develop and test recovery and contingency plans. IT governance is also important in ensuring a security program operates effectively.

² The cyber threats came from criminal groups, hackers and activists, insiders, nations, and terrorists. The cyber exploits included denial of service, malware, phishing, spamming and spoofing, structured query language (SQL) injections, and zero-day exploits. The cyber events included reconnaissance and information gathering, crafting an attack, delivering, inserting and installing malicious capabilities, conducting an attack, and exploiting vulnerable systems to gain access.

Federal laws and regulations (15 USC 6801, 45 CFR 160.103, 164.400-414,, 42 USC 1320d, Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule), and Hawaii Revised Statutes (Hawaii Revised Statutes 487N-1, Acts 135: Notification of Security Breaches, Act 136: Secured Disposal of Personal Identify Information, Act 137: Social Security Number Use Prohibitions) apply to the city's use of information technology and detail what data must be protected and the actions an entity must take when a breach occurs. The laws and regulations specify who must be notified, when the notices must be given, how the notices must be given, and enforcement actions and penalties that are applicable. Like other entities that have been breached, if an unauthorized access to city information systems occurs, the city will incur costs related to credit reports, identity theft protection, notifications, and other administrative costs.

Good information security programs follow up on identified threats; maintain coordinated communications within Department of Information Technology (DIT) and among city departments; and assess and validate security risks. Good programs document and implement security control policies and procedures; implement effective security awareness; monitor the effectiveness of the security program; and effectively remediate security weaknesses.

**Prior audit, consultant,
and financial reports**

Prior Audit Results: In January 2006, the *Audit of Selected City Information Technology Controls* (Report No. 06-01) stated the Department of Information Technology (DIT) oversight of security management was inadequate because DIT policies assigned oversight responsibility for security to the individual departments; risk assessments and monitoring were not implemented; and security was disjointed and not linked into a citywide security planning and management program. The report further stated DIT lacked sufficient authority to implement and monitor a citywide security management system; did not provide sufficient training on security; and needed to improve disaster recovery planning. The audit recommended that DIT develop a comprehensive IT security plan; obtain funding for a citywide risk assessment; and improve citywide security responsibilities. As a

³ The Department of Information Technology; Honolulu Police (sic, Police) Department, Honolulu Emergency Medical Services; and the Honolulu Fire Department. The critical issues found by the Presidio risk assessment are presented in Appendix E with their recommendation implementation status.

result of the audit, the department sought additional funds in its FY2007 budget to address the audit findings, and to procure the Presidio risk assessment for the city.

Presidio Consultant Results: The city commissioned the *City and County of Honolulu Risk Assessment* (May 27, 2009). The contractor, Presidio Networked Solutions of Greenbelt, Maryland reviewed four departments³ and provided a list of the top 10 critical findings and recommendations the city should address. The critical issues highlighted the need for an information security strategy; internal network security controls; centralized monitoring; information security monitoring; a comprehensive application security solution; and sensitive data on computers. The consultant recommended creating an information security organization with an executive level position responsible for strategic and tactical information security initiatives; implementing strong network security controls at key points in the network; and implementing a comprehensive network monitoring solution. The department implemented seven of the recommendations, including technical initiatives, such as acquiring a SIEM⁴ solution and implementing MPLS (see Appendix B) in the city's network.

⁴ Security and information event management (SIEM) systems are organized around the principle that the relevant data about an enterprise's security is produced in multiple locations. It consolidates that data to enable the ability to look at all security data from a single point of view makes it easier to spot trends and patterns that are out of the ordinary. SIEM combines security information management (SIM) and security event management (SEM) functions into one security management system.

Financial Information Audits Results: Prior financial information system audits by external auditors have repeatedly identified information system deficiencies in general and access controls⁵. These included concerns regarding physical and logical security, and change management. Over the last five years, annual repeat findings included the following:

- Several terminated employees continued to have access to the city's IT systems;
- No effective periodic review was performed to detect whether terminated individuals were able to log-on to the IT systems;
- No review was performed to determine whether access rights granted to employees were commensurate with their job responsibilities;

⁵ General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. The effectiveness of general controls at the citywide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the citywide and system levels, business process controls generally can be rendered ineffective by circumvention or modification.

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), and protect them from unauthorized modification, loss, and disclosure. Access controls include both logical and physical controls. It is fundamental that control techniques for both logical and physical access controls be risk-based.

Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute.

Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or exfiltrate (export) data or execute changes that are outside their span of authority.

- Lack of documentation and support for approvals that gave employees access rights to the IT systems; and
- Lack of segregation of duties (including areas of security administration).

The financial auditors noted that, collectively, the number and nature of IT control deficiencies resulted in an overall significant deficiency. They have repeatedly recommended that the city: update its IT policies and procedures to include internal control procedures that address the IT risks noted; identify methods to ensure that IT policies and procedures are consistently followed; and work with vendor programmers to address any internal control deficiencies due to the system limitations. In response, the department reported that they would make changes to internal control procedures, technical approaches, and monitoring to ensure policies and procedures are followed.

Audit and Consultant Issues Need to Be Resolved

Although DIT and the city implemented some of the audit and consultant Presidio recommendations, some audit and consultant issues still are unresolved. These are:

- Security management oversight needs to be improved. Responsibility for overall network system is assigned to DIT, but key security management oversight functions such as monitoring effectiveness, assessing risks, and evaluating impacts have not been implemented. Also, risk assessments at both the DIT and department levels are not performed or validated.
- Security training and awareness were limited; follow-up on identified threats and attacks did not regularly occur; a disaster recovery plan in the event of a cyberattack was needed; and the incident response plan was not tested.

Security at the DIT and department levels is not incorporated into a citywide security program. DIT staff need to follow up on identified threats, and communications within DIT and among city departments can be improved. Although the departments relied on DIT to provide security for their department IT operations, DIT security staff lacked sufficient authority to implement a citywide security program.

Security Management Oversight Can Be Improved

Good security management provides reasonable assurance that security management is effective by establishing policies and procedures that ensure periodic assessments and validation of risks; updated security control policies and procedures; and security awareness training and enforcement of security personnel policies. Other common security management practices include periodic testing, as well as evaluation of the effectiveness of information security policies, procedures, and practices; remediation of information security weaknesses; and periodic testing of security response plans.

Although DIT has responsibility for overall management of the city networks and cybersecurity, DIT assigned responsibility for key security management oversight functions (such as monitoring effectiveness, assessing risks, and evaluating impacts) to the individual departments. As a result, overall cybersecurity management and oversight at the department levels are inadequate and risk assessments at both the DIT and department levels are generally not performed or validated.

Although risk assessments are important for security programs, risk assessments were not performed

Risk assessments are important because they help identify threats and vulnerabilities; and provide a comprehensive starting point for developing or modifying an entity's security policies, plans, and programs. The risk assessment allows the city and its departments to identify and address the greatest risks, make appropriate decisions regarding which risks to accept, and which risks to mitigate through security controls and the security program.

The risk assessments are also important for identifying critical city data that must be protected. The risk assessment would identify data that federal and state laws require to be protected and allows the city to prioritize city data for protection. Based on the resources available, the city could identify and implement controls that economically, effectively, and efficiently protect the critical data from potential threats identified in the risk assessment.

The *Federal Information Security Modernization Act of 2014* (FISMA) provides a framework for managing risk, developing security policies, conducting security awareness training, and monitoring the adequacy of the entity's computer-related controls. Without these items, security programs may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Insufficient protection of sensitive or critical resources and disproportionately high

expenditures for controls over low-risk resources may occur without a well-designed security program.⁶

The National Institute of Standards and Technology (NIST) provides additional guidance on planning and managing an information security program. It has published a series of information security standards and guidelines for agencies to effectively manage risk to operations and assets, including minimum security requirements, standards for security categorization, and recommended security controls. It provides additional risk management guidance for applying minimum security requirements (see Appendix C).

An agency's risk assessment validates its security control set and determines if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), assets, individuals, and other organizations. The resulting set of security controls establishes a level of "security due diligence". A risk assessment starts by identifying potential threats and vulnerabilities, and mapping implemented controls to individual vulnerabilities. It then determines risk by calculating the likelihood and impact that any given vulnerability could be exploited, taking into account existing controls. The culmination of the risk assessment shows the calculated risk for all vulnerabilities and describes whether the risk should be accepted or mitigated. If mitigated by the implementation of a control, one needs to describe what additional security controls will be added to the system.

Our survey results and follow-up discussions confirmed over 64 percent of the city departments have not performed risk assessments or business impact analyses. During our review, we found the city currently lacked personnel policies related to IT security; IT security policies were outdated and obsolete; inadequate user awareness training provided; and no training on how to safely and securely use IT systems. Although information

⁶ The city's security program is currently inadequate because of incompleteness, despite its application of many IT technical security solutions. A common concern cited by department staff was the cost of providing IT security protection, these concerns about sufficient protection and cost of controls are valid, and may be better addressed with a more complete IT security management program which incorporates risk assessment, administrative guidance, training, and performance monitoring as a basis for evaluating security performance.

staff had identified security threats such as virus and system attacks to others, we found follow-up actions were needed to regularly communicate with the affected department, or to mitigate, prevent, detect, and correct the risks related to the virus attacks. As a result, security policies, programs, and plans for continued operations do not exist at the department levels. In our opinion, the unassessed security risks leave the city vulnerable and poorly equipped for protecting city and department information systems, data, and resources. For example, risk assessments would consider threats and vulnerabilities at the citywide level, department level, and information system and application levels. Based on the risk assessments, managers could develop strategies, plans, programs, policies, training, and controls needed to protect personnel data, financial resources, and accounting records. Without a risk assessment or business impact analysis, the departments cannot determine how to properly do their part in protecting their city information system resources, systems, or data.

Departments relied on DIT to perform the risk assessments and to protect their key systems, data, and resources

Our review showed over 64% of the departments did not perform risk assessments or business impact analyses for their information systems; took no action to protect their critical and confidential data; and took no actions to prevent unauthorized intrusions into their databases and computer systems. This condition existed because the departments relied on DIT to provide the policymaking and technical security needed to prevent the loss of their data and unauthorized access to their databases. That is, the departments were largely concerned about productivity, leaving IT security issues for DIT to resolve.

During our departmental surveys, the departments reported they considered DIT security administration as the focus and contact for the city's security efforts. The departments repeatedly cited DIT security administration as the party to contact to resolve or deal with security issues or problems.

The departmental reliance on DIT may be misplaced. Our follow-up discussions on the audit issues and consultant recommendations showed that formal citywide and departmental risk assessments are not conducted, and DIT lacked complete policymaking authority, including the ability to enforce DIT security policies, procedures, and processes.

The DIT staff and managers were not aware of the departmental level risks and operational vulnerabilities because no formal risk assessments or business impact analyses were performed. A current major DIT initiative is to improve the resiliency, security,

and reduce risks for the city systems by converting the city IT infrastructure and applications to virtual cloud operations. Recent incidents indicate the city's information technology systems are also a target for state sponsored attacks, hacktivist service disruptions, and loss of sensitive or critical data. Without a risk assessment, the major project implementation and the technical security approaches taken may not protect the city assets because DIT has incomplete information to effectively manage IT security and oversee the effectiveness of their current IT security management approaches to protect sensitive or critical data and systems. DIT needs the risk assessments to be aware of the threats posed (e.g., user behaviors, external attacks), or the impacts that may result from service disruptions or breaches (e.g. consequences and costs of breaches).



DIT did not perform risk assessments needed to plan and manage system security

The risk assessments were not performed by DIT although the city's 2007 *Cyber Security Incident Response Plan* states:

A sound approach to improving the organization's security posture and preventing incidents is to conduct periodic risk assessments of systems and applications. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. New threats and vulnerabilities are constantly emerging, and computer security is an ongoing process that requires diligence to be effective.

Regular risk assessments are needed to identify the types of information that need to be protected and to implement the appropriate security controls needed to protect the data. Without regular risk assessments, DIT may be unable to identify sensitive

and critical data, the range of risks that exist, and the necessary security measures that are needed.

The lack of regular risk assessment affects the ability of DIT to plan and manage the city's IT system security. According to IT security management practices, the results of an entity-wide risk assessment can be used to develop security plans from which IT implementations and operations can be secured in a manner consistent with the risk assessment and security planning. Security management and oversight then can be focused and organized around security planning objectives. The city currently does not perform risk assessments, and it also does not have a security plan. Without risk assessments, it cannot maximize the benefits from its IT security planning, and its activities may not reflect or appropriately defend the city's systems against current risks.

The DIT citywide security program also needs to improve and develop other supporting components needed for the security program: security awareness training; information system staff authorization to implement citywide information security measures; updated security control policies and procedures; and tests of city incident response plans.

Other Security Related Tasks Need to Be Addressed

We found security follow-up on identified threats and attacks could be improved; training and security awareness were limited; disaster recovery plan exercises concerning cyber attacks were not developed; and incident response plans were not tested.

Security awareness training is needed

The city does not have an actively managed, formal user awareness training or security personnel training needed to support and maintain a viable security program. Effective user awareness training and security-related personnel training are critical for effective security. Ineffective training can result in employees and city contractors inadvertently or intentionally compromising information system security.

Effective security programs normally consist of several elements. These include informing users of the importance of the information they handle; the reasons for maintaining system integrity and confidentiality; familiarizing them with security policies, procedures, and users' responsibilities; and providing security orientation, training, and refresher programs related to security guidelines.

Although previous audit and consultant reports cited the lack of security awareness training as a weakness, DIT and the city departments still did not routinely provide sufficient training on security personnel responsibilities, city security policies, security liaisons roles, and end user responsibilities and precautions.

DIT newsletter was primary security awareness tool

Currently, the DIT security administration section's security awareness efforts consist of primarily issuing infrequent newsletters related to cybersecurity, advisories, and general cybersecurity information. Although DIT security administration has been issuing the newsletters since 2011, the newsletters were irregularly published by the DIT administrator until the auditors pointed out how the newsletter could be used to improve security awareness to city users. During our audit, the DIT security administrator started to issue newsletters more frequently that promoted good personal computing habits and good behaviors related to system security; raised awareness on security issues and threats; and discussed unsafe security practices.

Although the intranet was a tool for archiving security policies, procedures, responsibilities, and expected behaviors, this tool was not used to provide security awareness or training to city users. Security staff acknowledged that the information posted was out of date, and was losing its usefulness. This information was also not easily accessible after the DIT migration to the current intranet. Without routine and frequent training or awareness, the city was at risk that authorized system users may compromise the security strategies and controls in place to protect city data, resources, and systems.

Follow-up process on identified threats needs improvement

Follow-ups on attacks, virus and malware identified, and enforcement of security policies and controls were not consistently performed according to policies or procedures. We learned through examples and demonstrations of technical security tools that even if DIT security administration staff had identified viruses and other malware, inconsistent follow-up actions to security alerts, lack of coordination or communication, or failure to follow through on enforcement or corrective actions may lead to unresolved false positive alerts or the unnecessary prolonging of real vulnerabilities and security issues. Consistent performance of technical security analysis, coordination, and communication are areas where improvements can ensure appropriate follow-up or enforcement actions are taken to maintain system security.

During our site observations and DIT security administration staff discussions, we learned that the city could be attacked by many methods. We understand that there is no 100% secure system, and that the application of security measures are intended to increase relative security. Common threats from hackers and cyber criminals include continuous scans for new or unprotected systems and software; distribution of malicious codes or infected items; tricking users to disclose security passwords; and phishing. Other threats originating from nation-states and hacktivist attacks could disrupt city IT systems and services. This is where consistent application of current technical security measures supplemented by prompt coordination, communication, and remediation activities can blunt or mitigate the effects of threats and attacks.



During our review, DIT demonstrated that the city faces ongoing cybersecurity threats to its network, systems, and resources. The DIT security administration staff showed via the monitoring conducted by its IT security devices that the city's systems were constantly being attacked from nations linked to malicious IT activities and cyberattacks. The department was alerted to two significant hacktivist threats (i.e. Vikingsdom and Anonymous) during our review. Both were designed to disrupt the State of Hawai'i website for publicity and to protest the 30-Meter Telescope (TMT) observatory project under construction on the top of Mauna Kea. The city was not affected by these attacks, but another municipal government in the United States did have its IT services disrupted temporarily, so these threats are credible and real. Also, on a daily basis, DIT security staff were alerted via monitoring devices to specific virus or malware activity affecting particular departmental networks and systems.



To supplement its technical monitoring with corrective action, the security administration staff notifies the customer service representative for the affected department to take measures to ensure these malware threats were removed, quarantined or deleted. This is the typical notification process for addressing a security problem involving departmental IT resources. During the demonstration, we found better threat validation and computer service representative (CSR) notifications were needed. Based on the demonstration, we concluded that malware threats were still active and residing on city computers four months after it was

identified by a security device and actions taken to validate or resolve the alert were incomplete.⁷

User security training is needed

A comprehensive security training, orientation, and refresher programs to train both new and existing employees and contractors on security guidelines did not exist. DIT recently started distributing the city's acceptable usage policy at new employee human resources orientation. The city also has a one-time acknowledgement of the security policy made at the time internet and email access privileges were granted, but no initial or ongoing training was provided.

A recent study has shown that careless and untrained insiders are an additional source of cybersecurity threats. However, organizations like the city still primarily focus security efforts on traditional external threat sources (e.g. external attacks on system perimeters and networks), and rely primarily on technical security devices and solutions for their system security.

Standard security management practices recommend that an ongoing security awareness program should be implemented that includes first-time training for all new employees, contractors, and users; periodic refresher training for all employees, contractors and users; and distribution of security policies detailing rules and expected behaviors to all affected personnel. Additionally, employees with significant security responsibilities or whose job involves information security should receive specialized training. Despite the importance of the security practices, the city does not provide initial or ongoing training on information security.

⁷ During a demonstration of a malware monitoring system in April 2015, we were shown an alert for a potential malware payload, and discussed the threat validation and notification process with security staff. The alert was generated in December 2014, and concerned potential malware on 20 computers in the city's transportation department. Security staff did not initiate the threat validation process, and no notification was sent to the affected department or CSR to remediate the potential problem. After further discussion, DIT believed this was a false positive alert, so no notification and remediation process was logged. However, they could not isolate the event to verify that this was so. To eliminate false positive alerts, the security staff will need to write a rule to ignore conditions that they have verified have no IT security consequence. They had not done so in this case.

Best practices of leading organizations consider promoting awareness to be one of the most important factors in managing the risks posed by authorized users and insiders. Awareness was considered to be especially important in reducing the risks of social engineering, where users are talked into revealing passwords or other sensitive information to potential thieves. Educating users about such risks makes them think twice before revealing sensitive data and makes them more likely to notice and report suspicious activity. Despite its importance, neither the city nor DIT are adequately promoting security awareness to reduce or manage the risks.

Users are not aware of system security

To comply with best practices, an agency wide information security program must include security awareness training for agency personnel, contractors, and other users of the information systems. The training should cover (1) information security risks associated with the users' activities, and (2) the user responsibilities for complying with agency security policies and procedures used to reduce the risks.

DIT did not routinely promote user awareness about IT security issues. Employee awareness is considered critical in combating security threats posed by spam, spyware, and phishing. While technical and administrative controls can aid in preventing or at least delaying many types of attacks, users did not receive training and were not aware of the threats identified by the DIT security staff, including:

- Spam (unsolicited commercial e-mail) consumes significant resources, and is sometimes used as a delivery mechanism for other types of cyberattacks.
- Spyware (software that monitors user activity without user knowledge or consent) can capture and release sensitive data, make unauthorized changes, and decrease system performance.
- Phishing (fraudulent messages to obtain personal or sensitive data) can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government services.

DIT also has not effectively used administrative means to communicate security awareness information within the city. We noted only two examples of citywide memos issued by DIT, both from several years ago, that focused on the key security threats

that confront users. The results of DIT security monitoring or technical assistance of departments could be communicated via administrative memos to inform department heads to reinforce and emphasize IT security with their staff. However, this method was not used by the department.

In response to our draft report, DIT staff initiated and distributed more frequent security awareness information throughout the city by issuing more frequent IT security newsletters and e-mail alerts.

Department users are granted access to systems or applications without security training

Based on our survey follow-up, departments do not require IT security training for users before they are granted access to city information systems. Security training ensures city users are aware of security system rules, user responsibilities, and acceptable user behavior. The Mayor's Directive 06-02 requires DIT to establish an ongoing comprehensive training program for DIT staff and users of the city's IT resources.

We found city departments were focused on productivity rather than security concerns. The most common criteria for access to IT resources was that users had the ability to operate computers and productively use the *Microsoft Office* suite of application software such as *Word*, *Excel*, *Power Point*, and *Access*. However, there was no training provided to ensure the secure or safe use of city IT systems.

Improved access management reviews can further reduce opportunities for unauthorized access

Best practices to monitor and control accounts require actively managing the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them. Previous audits reported, without regular account monitoring and adequate controls, terminated employees were able to access the city information systems although they no longer needed or were authorized access to city data, resources, or information systems.

The department utilizes certain automated account management controls to deactivate users, and reduce the window of opportunity for potential unauthorized access. These include the:

- daily automated job to disable inactive users in the city's human resources system;

- daily automated job to disable inactive new accounts that were never used for 30 days after being created; and
- daily automated job to disable accounts that have been inactive for 180 days.⁸

These automated methods are used in conjunction with manual methods to create, modify and terminate access to the city's IT systems and resources.

Our analysis indicates the manual management of access control can be improved. As demonstrated to us, the security administration staff also creates and modifies access to the city's IT systems and resources by manually processing e-form requests from user departments. They are heavily reliant on the departments to inform them when action should be taken to manage and oversee the accounts, particularly with respect to accounts that were subject to suspension, removal or deletion based on the employee status or lack of activity. As a result, dormant users not subject to automated termination were not deleted until the department submitted a request to deactivate the user's access. This is an ongoing security administration issue of balancing a reasonable duration of inactivity, while trying to prevent unauthorized access or control of these inactive accounts. As a result, the time between performing the manual processes and automated deactivations created a risk of impairing the security administration staff's ability to actively manage access to the city IT systems and to minimize the opportunities for attacks.

⁸ The department reports termination of employee access is a two-step process. When employees are set to inactive in the city's human resources system, their active directory accounts are automatically deactivated, making login impossible. The accounts remain in suspense until they are reactivated or moved into terminated status. DIT reports the reason for this is that some employees return shortly after being deactivated, or the department needs to reassign access to the deactivated account for research, litigation hold, or business continuity purposes. The IT purpose for keeping it in deactivated rather than moving immediately to terminated status is that, administratively, a terminated status would have to be re-entered to reactivate the employee.

Department requests to delete inactive accounts sometimes does not occur for years. When the requests and reviews were conducted by DIT security staff, the number of accounts to be terminated were in the hundreds. As a result, there is a risk that terminated employees, former contractors, and unauthorized users may be able to access, sabotage, destroy, delete, modify, or steal data that could affect city operations or assets before their access was automatically deactivated. For example, a non-city user conducting an accreditation review was granted access to city systems in August 2009. The department security liaison informed DIT in their initial security request that the accreditor's access was required for one week, and should be terminated at the end of that week. Six years later this account was still active. The account was subsequently included in a 2015 list of inactive accounts that should be terminated, with DIT requesting that the liaison confirm that this account was no longer needed.

During our review, we heard conflicting views as to when and how non-city user third party access was controlled. One staff member told us that third party access was only provided for a fixed duration. Another told us that the sponsoring department must request account closure. The department's director reported security administration over third party non-city users could be improved, and more could be accomplished in manual account access management and review, and working more closely with the departments who needed the third party users.

During the discussion of our audit results, the department reported fully implementing technical controls to improve their access management controls over inactive accounts. Despite the implementation, we believe this should be an area of active and continuous management concern, as previous financial audits raised concerns and issues about manual administrative reviews. A more proactive management approach can further improve control over these ongoing issues.

Contingency plans need to be tested

Current technologies such as mobile devices, project interfaces, third-party vendor oversight, the internet, e-commerce, and social media present challenges in protecting data and information systems. Current information technology standards state information systems should provide data when needed, confidential information should be protected (except when available through public sources), and information should have integrity. Information should also be available when needed, and comply with regulatory requirements. Deficiencies in these areas could affect city financial statements and adversely impact city decision making and city policies.

Currently cybersecurity-related attacks are more numerous and diverse, and can result in great damage and disruptive effects. New types of system attacks emerge frequently. Computer security incident responses have therefore become important components of information system security programs. A quick security incident response is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

In 2007, DIT's security administration section developed an incident response plan. The plan was established to handle and properly respond to cybersecurity incidents, such as service disruption, cyber-attacks, hacks, data breaches, viruses, spam, malware, and phishing. The plan established a standardized framework for coordinating the city's response to cybersecurity incidents, and to comply with payment card industry standards (PCI-DSS standards).

The plan was never tested. As a result, DIT does not know if it works or if it would mitigate any security incident such as a service disruption, data breach and theft of personnel data. Until the incident response plan is tested both internally and as part of the citywide recovery and continuity exercise, the effectiveness and validity of the plan is unknown.

The threat of a cybersecurity incident to disrupt city operations, services, or public safety is real, so testing response capability is appropriate and necessary. City also needs to conduct its own penetration tests or "red team" exercises to test the strength of DIT defenses through simulated attacks. Without these tests, the city cannot determine if its cybersecurity defenses are valid, appropriate to the threats, and effective.

During our discussions, DIT reported the department had the capability to conduct penetration tests, exercises, and simulated attacks. However, there was no evidence these exercises had been conducted as a part of its operations.

Security standards recommend regular testing of incident response plans

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (February 2014), identifies guidelines for agencies to test their incident response capability, and to determine the effectiveness of the security incident response procedures. Agencies should also train personnel in their incident response roles and responsibilities. According to NIST, the lack of a well-trained and capable staff could result in ineffective incident detection, incorrect analysis, and costly mistakes.

The DIT security administration section has not conducted exercises to test its ability to respond to IT security incidents. According to NIST, organizations should be proactive and educate its staff and users about important security controls, regularly test its security, and update its incident response plans. Drills ensure everyone understands their roles and responsibilities and know what to do to respond quickly and correctly. Updated drills and plans ensure the response plans work. Common exercises include table top exercises to run through the incident response plans. Depending on the risks or threats, some organizations should practice monthly on possible scenarios and revise the plans to eliminate mistakes identified during the drills. The drills prepare and help determine if in-house resources are able to effectively neutralize the most likely threats, and whether additional assistance is needed.

By not testing the DIT plans, the city has no assurance the existing security defenses are effective in protecting city information systems, resources, and data. By not testing and exercising the incident response plans, DIT cannot ensure the city costs related to a breach and the data lost are minimized.

DIT needs to plan for compliance with additional future PCI requirements

The Payment Card Industry - Data Security Standards (PCI-DSS) were created due to increasing losses due to credit card fraud. The new PCI-DSS industry standards place the burden for protecting credit card and customer data on the entity that collects the data. The data is usually collected by the city at the point of sale or payment, including on-line and at the payment counter. According to PCI-DSS requirements, if a breach occurs and critical data such as personal identity information (such as birthdate, names, social security numbers, and personal data not generally available to the public) are stolen, the city may be liable for any losses and any investigation costs. These costs are in addition to the notifications, credit report, identify theft protection, and other administrative costs mandated by federal and state laws.

The city has future plans to accept payment cards for certain city services. In its planned expansion to accomplish this, the city must build and maintain a secure network and system; protect cardholder data; and maintain a vulnerability management program. It also must implement strong access control measures; regularly monitor and test networks; and maintain an information security policy. The standards apply to all entities that store, process, or transmit credit cardholder data.

The DIT director reports that currently the city has a limited scope for PCI-DSS compliance, and that transactions occur with

payment processors and banks with no data being held or passed through the city's systems and networks. Currently, this may exempt the city from being compliant with certain PCI assessment criteria, and only requires the preparation of an incident response plan (PCI-DSS 12.10.1). However, the director did acknowledge the need to put more emphasis on PCI-DSS compliance due to the city's future plans. We concur that this is needed.

At this point, the city would not be in compliance with an expanded PCI-DSS assessment, and would be at risk for considerable losses should a breach occur without addressing the following points in the future. In response to our concerns and our draft report, the city is currently considering technical solutions to comply with these standards and to accomplish its future plans of accepting payment cards for certain city services.

As a result of our audit discussions, DIT reported that it will test and update its incident response plan in 2016. It is also currently considering technical solutions to comply with these standards and to accomplish its future plans of expanding acceptance of payment cards for city services.

City's cybersecurity incident response is untested

Standards for continuity planning recommend that organizations should ensure that incident response policies, procedures, and business continuity processes are synchronized. The standards state computer security incidents may undermine the business resilience of the organization, and business continuity planning should consider security incidents and their impacts. That is, business impact assessments, risk assessments, and continuity of operations plans should be adjusted as needed to minimize operational disruption during severe circumstances, such as cybersecurity attacks, denial of service, and other attacks.

DIT holds an annual disaster recovery exercise to test the city's capability to recover from a disaster and to test its readiness to support disaster preparedness, business continuity, public safety, and city services in the event of a major disaster. The test involves activating the DIT secondary data center in Kapolei in order to recover and resume city IT operations in the event of a disaster or failure of the city's primary data center.⁹

⁹ During our audit, DIT reported it approached these incidents according to its disaster recovery plans and exercises, and recovery excluded cyber security functions.

DIT has never tested response to a cybersecurity incident. Currently, the DIT cybersecurity incident response plan is over eight years old, and may be obsolete. Without testing, DIT is unable to discover deficiencies in its planned incident response, and cannot determine if the response plan is adequate or relevant to the current threats.

Better City Security Coordination Over Its Policy Framework is Needed

Technical security at DIT is centralized, but the integration of its governance with the departments via its current policy framework is not well coordinated to support a citywide security program. At the department level, key security management oversight functions such as monitoring effectiveness, assessing risks, and evaluating impacts have not been implemented as part of a citywide program. As a consequence, the departments rely on DIT to provide security for the department IT systems and resources although DIT lacks sufficient authority to implement the policy framework required of a citywide security system and its support is largely limited to technical support.

During a survey of IT systems and security policies among 17 city departments, we found that most of the departments had not performed risk or business impact assessments or identified security threats; and did not have security policies - although most did have business continuity plans if an event occurred. Some of the departments stated they relied solely on DIT to perform cybersecurity tasks and to protect their information systems and data.¹⁰

Although the department tasks were established by city security policies and plans as measures for an effective and successful citywide IT security, our audit results showed the departments were inconsistently performing planning or policymaking tasks. Most were relying on DIT to ensure their security, or to coordinate improvements when needed. DIT, however, was not monitoring or coordinating the performance of tasks or the overall policy to ensure the city's cybersecurity was effective and appropriate. These policies have also not been updated for a long time, and made their relevance to current IT operations and systems questionable.

¹⁰ According to the Presidio report, DIT is responsible for security services such as Web Filtering, Remote VPN Access, Firewalls, SPAM filtering, and Anti-Virus. Although not complete, the list represents the level of critical services that city departments rely on from DIT.

Exhibit 2.1**Office of the City Auditor, Information Technology Systems and Security Policies Survey Results**

Survey Question	Survey Results	
	Yes	No
Has the department developed its own IT policies (e.g. user, IT security, and internet policies)?	5	12
Has the department identified and assessed IT security threats to its critical systems and data, and determined ways to eliminate or control these threats by developing an IT internal risk assessment?	6	11
Does the department have a business continuity plan to ensure operational business functions and data protection in the event of an IT infrastructure outage or security event?	9	8

Source: Office of the City Auditor

Updated security control policies and procedures are needed

An effective security program requires that security policies and plans should be maintained to reflect current conditions. It should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk, mission, types and configuration of the computer resources used. The revised policies and plans should be reviewed, approved, and communicated to all employees. Policies and plans should reflect current risks and should be applicable to the existing cybersecurity program.

Prior to 2015, the overall set of IT policies and procedures had not been updated for years, despite being a responsibility of DIT security per the current Mayor's Directive 06-02. By not updating and maintaining policies and procedures that reflect current conditions, the city did not have a complete and effective set of policies and plans that reflected changes to risks, performance objectives, and the current state of the city's IT systems and operations. Some existing security control policies and procedures still need to be updated. Exhibit 2.2 lists the latest information system security directives.

Exhibit 2.2 State of Current IT Plans and Policies

<i>Name of Plan or Policy</i>	<i>Purpose</i>	<i>Implementation/Latest Version</i>
Mayor's Directive 06-02, Policy on Information Technology Services	This directive establishes the general policy on Information Technology services for the City and County of Honolulu.	January 2006
Cybersecurity Incident Response Plan	The purpose of this Incident Response Plan is to establish a standardized framework for the City and County of Honolulu's response to cybersecurity incidents.	July 2007
City and County of Honolulu Cybersecurity Plan	This is a five year Cybersecurity Strategic Plan that outlines the City's goals and strategies for securing the City which is centered on building collaboration, reducing risk, increasing cybersecurity awareness, and developing a secure architecture for information sharing.	September 2007
Acceptable Usage of Information Technology Resources*	To establish an acceptable use policy to ensure that information technology resources are being used in an effective and efficient manner	October 2015

* The previous city policies concerning its Internet Policy and Guidelines and General Information Technology Security Policy have been replaced by the Acceptable Usage of Information Technology Resources as of October 2015.

Source: Department of Information Technology

We found that:

- The Mayor's Directive, Policy on Information Technology Services, will be ten years old on September 2016. Since the issuance of this directive, there have been three mayors and no revisions to this policy, even though the city and the general IT environment have changed (e.g., CHERPS, Internet-based customer services).
- An incident response plan requires a process to modify and evolve the plan according to lessons learned, testing or actual events, and current security developments. The plan has gone over eight years without revision or testing, so there is no assurance it is appropriate and effective for the current security environment.

Although updates are frequently made to its technology road map and an acceptable use policy has been recently issued, the department has not regularly reviewed and updated its security

policies and plans to reflect changes in its risk, mission, and the current computing environment.¹¹ Regular review and policy updates can help management to understand and evaluate security risks; develop, maintain and monitor plans and policies to make the security management efficient and effective; and bolster the commitment to system security. Outdated cybersecurity and incident response plans may reduce the ability for management to respond appropriately to cybersecurity risks and threats.

According to IT security management standards, over time, policies and procedures may become inadequate because of changes in threats, changes in operations or deterioration in the degree of compliance. Therefore, periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to security. Such assessments should be performed by DIT security staff, but none currently are performed.

Based on the draft audit report, DIT reported that the security section has been tasked to review and update the policies and procedures. Also in response to the draft audit report, DIT developed a draft security awareness and training program plan in March 2016. The draft plan will need to be officially approved before it can be implemented on a citywide basis.

Recommendations

The Managing Director should direct DIT to:

1. Conduct periodic risk assessments of systems and applications to improve the organization's security posture and prevent incidents;
2. Create a citywide information user security awareness training that includes all users of information systems, external non-city users, and others who support the city's IT operations and assets;

¹¹ DIT uses a technology roadmap to master plan its significant IT projects in support of its overall strategic direction and vision. This document is updated every two months and is included in Appendix I. In 2015, the department issued a citywide acceptable use policy to ensure productive use of the city's IT systems. It plans to implement a user acknowledgment of this policy as a condition of being granted user privileges.

3. Require security awareness training before anyone is permitted to access city information systems or applications, and include, but not be limited to, information security risks associated with users' activities; users' responsibilities in complying with city and department policies and procedures designed to reduce these risks; and training of personnel with significant responsibilities for information security;
4. Consider integrating information security concerns into human resources policies, particularly with respect to hiring, termination, and disclosure of sensitive information;
5. Improve access management by reducing reliance on manual methods and establishing timelines for department notifications to the DIT security administrator;
6. Review, assess, and implement cybersecurity controls that are appropriate and cost effective for immediate implementation and add value to security initiatives;
7. Regularly test incident response plans and develop an incident response program that plans, provides, modifies, and accommodates changes in the IT computing environment;
8. Develop and address PCI-DSS requirements before activating future plans for e-commerce and on-line transactions; and
9. Update security control policies and procedures.

Chapter 3

DIT Security Staff Needs Authority to Implement Security Measures

Security deficiencies exist because information security staff lack the authority to implement citywide security measures. Security weaknesses can be remediated and a citywide security approach for remedial action is possible if a chief information security officer is established as recommended by previous consultant and audit reports.

Background

The Council on Cyber Security identified 20 critical controls for an effective cybersecurity program. These were:

1. An inventory of authorized and unauthorized devices;
2. An inventory of authorized and unauthorized software;
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;
4. Continuous vulnerability assessment and remediation;
5. Malware defenses;
6. Application software security;
7. Wireless access control;
8. Data recovery capability;
9. Security skills assessment and appropriate training to fill gaps;
10. Secure configurations for network devices such as firewalls, routers, and switches;
11. Limitation and control of network ports, protocols, and services;
12. Controlled use of administrative privileges;
13. Boundary defense;
14. Maintenance, monitoring, and analysis of audit logs;

15. Controlled access based on the need to know;
16. Account monitoring and control;
17. Data protection;
18. Incident response and management;
19. Secure network engineering; and
20. Penetration tests and Red Team exercises.

The report also identified 23 attack types and the critical security controls needed.

Information Security Staff Lack the Authority to Implement Security Measures

As discussed earlier, the city and its DIT processes need to ensure critical controls are followed for the benefit of secure city IT operations and public service. For example, we were made aware of instances where DIT security administration staff had apparently identified or were informed of IT security issues, but the information and follow-up action with other DIT sections and other departments was incomplete. Follow-ups on attacks, identification of viruses and malware, and enforcement of security policies and controls were incomplete because the DIT security staff lacked the authority and responsibility to ensure remedial actions were taken, or that monitoring and evaluation would result in appropriate corrective changes. Without this authority, the security staff had limited ability to protect city data assets from hacking activities and limited responsibility for minimizing city data losses and costs related to any data breaches.

According to the DIT security administrator, the information security job was basically the same as his predecessor and lacked the authority, responsibility, or leadership support needed to successfully implement a comprehensive, citywide IT information and cybersecurity program. As a consequence, citywide security initiatives outside the scope of technical support services were difficult to achieve.

Current DIT security activities are limited to technical and administrative tasks

The DIT security administrator is in the Technical Support division. As security administrator, the primary security functions currently include:

- user administration – creating and authorizing users and groups
- e-forms security – monitoring and implementing user passwords and login
- perimeter control – maintaining the city’s internet and intranet firewall
- response to suspicious or malicious events – monitoring the antivirus gateways, and performing security event monitoring

These administrative tasks compose the majority of the security administration staff’s daily work.

DIT lacks the authority to enforce information security policies at the departmental level. DIT security staff therefore limit their communications with other departments to an “as needed” basis. Their primary operational focus is providing technical security controls for the external perimeter of the city network, defense of the city network, and administering access to accounts. The DIT security staff leave responsibility for IT security policymaking¹, monitoring users and enforcement, and assessing risks and impacts to each department. The individual departments are considered to be the first line of internal defense, and are expected to implement and enforce their own appropriate security policies.

The DIT security administrator function is not equivalent to other chiefs of DIT functional groups or divisions although the security function has citywide implications and touches everything the city does regarding information technology. The DIT security administrator lacks the autonomy and ability to make decisions on resources and staffing.

¹ DIT allows departments to implement additional policies if the DIT policies are not restrictive enough for them. The most recent instance is the Department of Human Resources policy on protection of personal information (which includes electronic information) to comply with the state law concerning identity theft prevention.

The current responsibilities of the security administration do not reflect the roles defined by information technology operations standards. These standards indicate that cybersecurity is highly dependent on the commitment of management. That is, management must understand and evaluate security risks, enforce security policies and procedures, and maintain security standards. Typically, a security administrator also does the following:

- Maintain access rules to data and other resources;
- Maintain security and confidentiality over the issuance and maintenance of authorized user IDs and passwords;
- Monitor security violations and taking corrective action to ensure that adequate security is provided;
- Periodically review and evaluate the security policy and suggest necessary changes to management;
- Test the security architecture to evaluate its strengths and detect possible threats; and
- Prepare and monitor the user awareness program.

According to prior consultant and audit reports, DIT needs to create an executive level position to implement citywide strategic and tactical security initiatives, expand the role of DIT security, coordinate security with other departments, and obtain the staff, security and technical personnel needed for the security program. Absent the executive position, the typical citywide IT security management activities are difficult to implement, and are subject to shifting priorities of the department.

DIT needs to prioritize security management to protect city information resources

To improve security against increasing threats, DIT security staff must have the authority, as well as, the responsibility to implement security practices, policies, and practices needed to protect city information systems, data, and resources. More specifically, the DIT security staff should have the authority to:

- develop and enforce compliance with the security strategy;
- ensure risk assessments are conducted;
- ensure security gaps and overlaps are identified and addressed;

- oversee the security program and initiatives;
- develop risk mitigation strategies;
- develop and implement security monitoring activities;
- develop performance metrics; and
- enforce security policies, procedures, and processes.

Typically, the authority and responsibility for the above IT security management functions are assigned to a senior management position such as a chief information security officer (CISO), who has the appropriate authority and responsibility to perform these activities.

Previous security administration initiatives affected by lack of administrative priority

The DIT security administrator prepared a 5-year cybersecurity strategic plan in 2007 that provided the city's goals and strategies for securing the city, building collaboration with external parties, reducing risk, increasing cybersecurity awareness, and developing a secure architecture for information sharing. The plan itemized cybersecurity initiatives and projects over the 5-year period needed to achieve the plan goals.

We found many of the projects were not completed and the overall goal was not attained. Items completed were those under the control of the DIT security administrator. Items not completed were due to inadequate support, communications, and other priorities within DIT. For example:

- The previous DIT director wanted to implement a single sign-on (SSO) and user self-service solution from a vendor without properly establishing the number of user licenses required and without obtaining the full funding needed for the project. Although a license was required for each user, only 1,000 of 10,000 licenses were bought. As a result, the project languished on the project list for five years and was not implemented until the new DIT director was appointed in 2013 and implemented an effective single sign-on program.
- An infrastructure project for coordinating multiple parties through an external extranet application was not implemented because the DIT director was not supportive of the project, and department communications did not explain the feasibility and importance of the project.

To improve security against increasing threats, DIT security staff or its administrator must have greater authority, as well as, the responsibility to implement security practices, policies, and practices needed to protect city information systems, data, and resources.

Critical security controls for an effective cyber defense are incomplete



Source: Office of the City Auditor and Council on Cyber Security

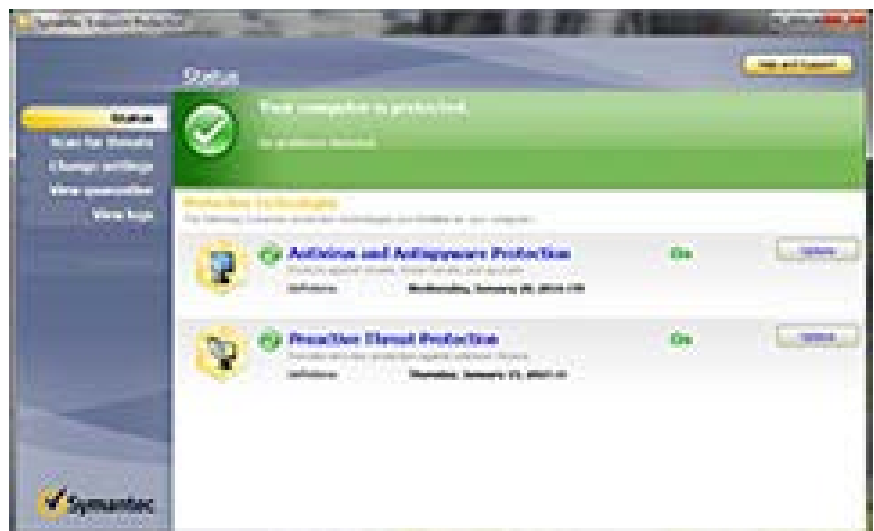
Although DIT cybersecurity operations partially implemented 19 of the 20 recommended critical security controls, DIT and the city departments lacked a complete strategy, plan, or program for fully implementing these suggested critical security controls and for preventing the 23 attack types identified in the report.

DIT security reports that it attempts to apply *best of breed*² technical security devices, but its security operations are reactive and are not managed to proactively prevent, detect, or correct cyber-attacks. In our opinion, DIT’s selective application of controls in its operations, without risk assessments may affect the department’s ability to limit data losses and minimize city costs should a hack or data breach occur.

² Best of breed security devices are the best product of its type. In the IT environment, organizations often purchase security solutions from different vendors in order to obtain the best-of-breed for each area. For example, it may buy a security event information management device from one vendor, and a malware endpoint solution from another. Integrated security management solutions are available from single vendors, but every component may not be best-of-breed, since it is difficult to excel in every niche.

More specifically, we found the city's partial implementation of the 20 controls featured incomplete controls and other potential weaknesses, which may have serious IT security implications for the city. More specifically:

- ***Authorized vs. unauthorized devices and software:***
The city has the ability to inventory authorized and unauthorized devices and unauthorized software, but currently does not actively manage (inventory, track, and correct) this capability. Its approach is to use this information only as needed to react to certain situations. Active management of these controls is regarded as an essential control for all IT security programs. As a consequence, the city:
 - ✓ Cannot ensure that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access to city systems.
 - ✓ Cannot ensure that only authorized software is installed and executed, and that unauthorized and unmanaged software is found and prevented from installing or executing actions on city systems.
 - ✓ Is unable to find systems running vulnerable or malicious software; mitigate problems; or root out attackers. As a consequence, malware may exist on city networks or resources for months.



- **Malware:** Another essential control is malware defense. The city applies a defense-in-depth approach to malware protection, which includes the desktop, Internet and network connections, and email gateways. We found that:
 - ✓ The previous malware protection software on the user desktops reached its end of life in December 2014 and was no longer supported by the vendor.
 - ✓ Zero-day protection on desktops was not updated until February 2016, 14 months later. Zero-day protection is the ability to provide protection against zero-day exploits, which are generally unknown to the public, and difficult to defend against. Zero-day attacks are often effective against “secure” networks and can remain undetected even after they are launched.

Other potential weaknesses included the following:

- Responsibility for application software security was passed from the security administration section to the applications division. The city has purchased application scanning solutions, but currently has not implemented processes to ensure applications and services are secured before being put into production. The intent of the application software security control is to manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. Attacks often take advantage of vulnerabilities found in web-based and other application software. Leading security practices suggest that it should be a shared responsibility to maximize application security rather than to belong to one function or the other.
- Sensitive information is not protected using data loss prevention (DLP)³ solutions to prevent exfiltration (export) of sensitive data. In our opinion, sensitive information was not properly protected because this security control was not implemented.

³ *Data loss prevention (DLP)* is a strategy for making sure that end users do not send sensitive or critical information outside a network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

Data exfiltration is the unauthorized transfer of sensitive information from a target’s network to a location which a threat actor controls.

Remediation of Security Weaknesses Is Needed

An organized approach is required when cybersecurity weaknesses are identified and remediated. Although DIT has some activities in place to assess the city network vulnerabilities, patch and upgrade deficiencies, and deal with identified security weaknesses, DIT security controls to remediate weaknesses are reactive and not well planned or organized.

A citywide approach to cybersecurity does not exist

We found DIT does not have a comprehensive cybersecurity strategy or an overall program for protecting the variety of devices, databases, and applications used throughout the city. For instance, the city lacks a security program that details DIT and city department roles and responsibilities; identifies major systems, databases and facilities; designates who is responsible for managing security for the different systems; and who owns, uses, or must protect specific systems, data, and other resources. Without the above information, the ability of the city's information security program to protect city data is limited.

DIT uses a mix of automated and manual processes to remediate security activities

The security administration section currently uses a mix of automated and manual processes to identify and remediate security issues, and remediation actions are not planned or organized programmatically. According to security standards, DIT remediation actions should be planned, and organized procedurally and programmatically (e.g., identify, assess, correct, and monitor). Plans and milestones should be based on security control assessments, security impact analyses, continuous monitoring activities, audit reports or other reliable information. Currently, the security administration section does not adhere

to any security management standards or frameworks to define its operations. Rather, the security administrative staff picks and chooses among selected practices, and as appropriate, applies some best of breed devices and software to assist with its technical security operations. They currently deal with IT security issues, weaknesses, and problems reactively as they occur. There are no action or corrective plans, set programs, or processes to approach remediation.



The following discussion of examples does not imply that the sum of department IT security efforts are deficient, but point out that there are issues in the current approaches to remediation involving administrative activities, communication and

coordination, and incident handling. No matter the technical solutions applied, these examples are security situations that require active, consistent management and review. If the few examples here are more commonplace than the department currently believes, the city is highly vulnerable to the effects of security events and incidents in ways it does not currently anticipate.

Remediation efforts were incomplete during process demonstration

The DIT security staff demonstrated their security processes used to remediate the effects of a malware payload on computers on the network. The staff member demonstrated how they would be alerted to potential malware on the network, and how they validated whether there was a malware component. If there was a malware component, the security staff sends an email to the affected department's DIT Customer Service Representative, the DIT Help Desk, and the police department. The department and the customer service representative were expected to scan computers and run antivirus to eliminate or quarantine the malware. The customer service representative was supposed to inform the security staff that the antivirus was run, and report that the incident was resolved (closed out).

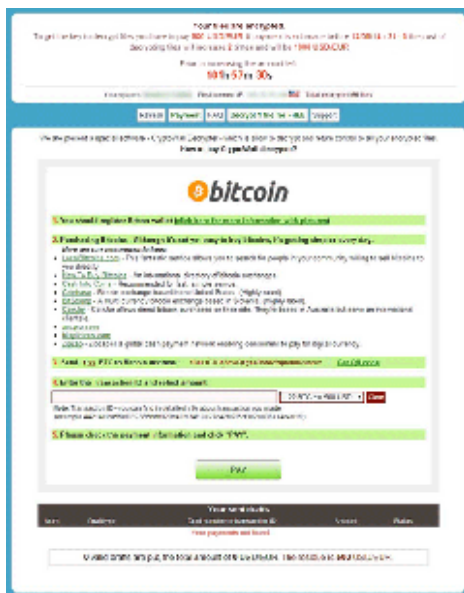
During the demonstration, despite a listed malware alert, the DIT staff member told us he did not think there was anything to demonstrate because he believed all current network malware threats were neutralized and the infected computers were cleaned. The staff member went to the Internet to determine if there was malware associated with the alert that 20 computers were potentially affected. The result of the scan was the highest risk of malware. The surprised security staff member insisted the malware was already mitigated and the computer was cleaned. After consulting a spreadsheet for detected malware information and dates, there were no emails sent to the department or confirming emails received, so the malware problem was still open. As a result, we concluded that the malware payload was still sitting on 20 machines in the department and four months had elapsed from the alert (December 2014) to the demonstration date (April 2015).⁴

⁴ After discussion of this finding with security staff, they could not isolate this event based on our information to verify the situation. From the information presented, staff reported that this was likely a false positive alert. To deal with false positive alerts, staff normally writes a rule to exclude it from recurring. In this case, no rule was written to turn off the alert. In the staff's opinion, this was why there was also no record of communication with the computer service representative or efforts to remediate this situation during the demonstration.

In our opinion, the consistent application of standard validation procedures and notification processes, standard citywide follow-up tests, and frequent follow-up reviews would have resolved the malware alert (or problem) sooner. Also, to improve its response, staff needs to perform its routine administrative activity to remove false positive alerts in order to reduce the number of alerts to actionable alerts that require response and coordination. It had not done so for the incident related to the demonstration.

A second case study shows failure to follow-up resulted in loss of critical data and work

In a second case, the security administration's monitoring of technical security devices did not prevent the loss of critical data and work performed by a city employee. The DIT automated security information monitor was alerted that ransomware was found on the city system. DIT security devices identified the situation, and normally the city's proxy server would automatically drop the connection before any computers were infected. What security staff did not know was that the user's computer had its proxy setting off, which was discovered in the subsequent review of what occurred.⁵



The city does have security and networking tools that provide visibility and attribution, identify the affected agency, and identify the affected user's proxy state. We understand that these tools identified the security situation with the ransomware. However, security did not ask the assigned DIT CSR to alert the affected city agency to take precautions and did not attempt to prevent or avoid the situation.

The result of this incident was that a user's computer hard drive and an external, detachable hard drive connected to the computer were infected by the ransomware, *Cryptowall*. This particular ransomware encrypts all files until a monetary ransom is paid to unlock them. The ransomware infection could not be resolved, destroyed the user's files, and two months of work was lost.⁶

⁵ In October 2014, the security section issued an advisory after this incident. It contained steps that users should take to ensure their systems and activities are secure. The user security steps should have been the subject of user awareness bulletins before the incident occurred.

⁶ The department reported taking post-incident recovery action to send the disk for forensic analysis. This was unsuccessful. DIT reports there is not much that can be done once files are encrypted by ransomware.

In our opinion, if the security section had applied its typical notification process, the situation involving the particularly destructive nature of ransomware could have been mitigated. Increased user awareness and better security staff coordination and communication may also prevent similar incidents, similar adverse results, and similar damage from occurring.

A third case shows internal threats exist

In a third case, a disgruntled employee with a grudge sent malware to another user in his agency via an e-mail. The email was mass-addressed to various employees in the agency and infected a large number of computers. An affected office notified security that this occurred so remediation of the malware could start.⁷

The DIT security section has a process to issue alert notifications when these situations occur. DIT reports that issuing an alert depends on how many users are affected, and whether the threat has been contained. No notification resulted from this event. The lack of any alerts or notifications in both cases and the lack of proactive security actions resulted in the infection of city computers with malware and the loss of critical data and productivity.

A fourth case shows inappropriate protection for confidential files

In a fourth case, after changes were made to the system, a division's confidential collection of files on the city's document management system were accessible to unintended users within the same agency due to the setting of improper permissions. The files could be accessed by those with knowledge of a specific account ID and password commonly known within the agency.

Prior to the changes, the affected division chief asked DIT to carefully re-consider permissions to its confidential collection because of the way overall agency permissions to certain collections were organized. The permissions were not reviewed and an account which belonged to another division in the agency was inadvertently linked to the confidential collection. The affected division discovered this situation internally, and asked DIT to review if this was the case. In a memo to the affected

⁷ During our audit, DIT reported 13 instances in 2013 where alerts were issued. After upgrades were made to the email gateway security in 2014, DIT reported no incidents warranted issuing alerts.

division, DIT estimated that the situation persisted for nearly six months before the permissions issue was resolved. The affected division remains concerned about the effects of any confidential information and data that was possibly accessed.⁸

In discussions, DIT reported correcting the issue quickly after being notified.

According to the Mayor's Directive 06-02 and the city's security policy, the department is responsible for prohibiting unauthorized access to city-owned computer resources, and for overseeing and enforcing against unauthorized access to the computer network systems controlled by DIT security. DIT was in charge of making changes to the permissions, but did not review permissions, or consult the affected division to confirm permissions were set up appropriately for their operational needs.

This case shows that inadvertent mistakes and oversights may occur through reliance on technical solutions alone. That is, user agencies should be consulted throughout the implementation process to disclose what is planned, so they can review and identify that intended permissions are in effect, and that unintended permissions can be quickly addressed and removed prior to implementation. Insight into the agency's perspective of suitability for its operations cannot be determined without this communication and coordination. In this situation, the security issue was not discovered for many months, and its exposure, while assumed confined to a limited set of internal users, is really unknown.

A citywide security approach for remedial action is needed

Standard security practice is to apply information from the remediation process to adjust or modify citywide cybersecurity policies, practices and procedures, and to help management to determine the adequacy and effectiveness of the security program and practices. When standardized, it can be used to produce significant performance information that can be used for reports such as annual reports, budgets, and management plans. If

⁸ DIT estimated the potential exposure was only to those agency users who knew the ID and password of the account. Although the damage was limited, DIT reported it had no way to determine if permissions were changed or who accessed certain files because the city's document management system does not log that kind of information. In response to this situation, DIT reported it now submits an access list and current permissions to departments for their review prior to any permission changes. This is used as a compensating control.

implemented properly, the security program can also serve as the basis for budget and staffing requests, support performance plans, and to quantify the time and resources needed for the security program.

The city currently lacks a process for planning, implementing, evaluating, and documenting remedial actions. For example, deficiencies in information security policies, procedures, and practices are not identified and addressed; processes for handling threats and security vulnerabilities through automated or manual processes are difficult to assess; and follow-up actions are not assured. Before significant attacks occur, DIT security staff needs to ensure security deficiencies are adequately remediated. For instance, DIT security staff needs to ensure the DIT remediation process is used to adjust or modify citywide cybersecurity policies, practices and procedures, and used to help management determine the adequacy and effectiveness of the DIT security program and practices. These improvements would help to protect city information systems, data, and resources from internal and external attacks, hacks, and breaches.

A Chief Information Security Officer Is Needed

The *City and County of Honolulu Risk Assessment* (May 27, 2009) by Presidio Networked Solutions of Greenbelt, Maryland recommended creating an information security organization with an executive level position responsible for strategic and tactical information security initiatives; implementing strong network security controls at key points in the network; and implementing a comprehensive network monitoring solution.

The Presidio report expected the executive position to fulfill several functions. These included developing a security strategy; implementing information security projects; and providing leadership in the security program. The DIT executive level position was needed so someone would be responsible for security initiatives, coordinating security within DIT and with the other city departments, and providing resources such as technical security personnel for the security program.

Lucent NetworkCare issued the 2000 report, *High-level Security Assessment Executive Summary for City and County of Honolulu*. The report recommended the creation of an executive level information security officer because the city did not have one and the Mayor's Directive appeared to cause problems such as gaps in its security framework; no citywide security plan; no formal data classification policy; no alignment of strategy, plans, and policies; and lack of enforcement of the city's security policy.

City still needs an executive level official responsible for security

Despite previous recommendations for independent assessments, previous DIT directors chose not to establish an executive level information security officer (chief information security officer – CISO) and kept the executive role and responsibilities for security with themselves. The current DIT director is the city’s chief information officer (CIO).

CIO Magazine suggests that information security is a necessity rather than a luxury today. For the longest time, information security was within the purview of the CIO, another duty in a long list of existing responsibilities and job requirements. This traditional assignment may result in inattention to security.

CIOs may have so many projects, problems, and plans that they may neglect their responsibility to bolster the security profile of their systems and monitor the integrity of their networks and systems. They also may not have the technical expertise or continuing education required to stay on top of security threats and the evolving nature of the security landscape.

To appropriately deal with the situation, it is advised that an executive role be created to focus solely on security. A CISO should be charged solely with managing the current security profile, and ensuring that the hardening of networks and systems continues at an effective and efficient pace. It would have the authority and budget to respond to incidents quickly and efficiently.

In the case where the CIO has ambitious plans to do many things and proceed with a lot of projects – as does DIT currently, the CIO may not have fully considered the security implications entailed. They may not have security expertise, but also it puts the CIO in the oddly unrealistic position of advocating against their own plans and projects due to security reasons. Ideally, a CISO would have the responsibility to rigorously evaluate the plans, the intended services and uses; validate it from a security perspective; request revisions to mitigate issues; or veto a project if a serious issue cannot be practically remedied.

Without the independent role, security efforts may not resolve the reported issues and deficiencies, and practically it may not achieve planned objectives (e.g., department’s 2007 cybersecurity 5-year plan). More specifically, the city and DIT still lack a comprehensive security strategy and program; existing security policies are not enforced; existing staff efforts are not prioritized and used to resolve security deficiencies; and staffing is focused on ensuring the city operations are available 24 hours a day and 7 days a week instead of integrating security throughout its

operations to protect the city data, resources, and intra- and inter-networks.

Without a chief information security officer, the city and DIT is unable to designate anyone with the authority and responsibility for creating, managing, monitoring, and improving citywide security. As a result, the city lacks overall planning, training, and awareness programs related to cybersecurity issues; and staff assigned to security functions cannot provide technical support needed to protect the city data and resources. The absence of the executive level chief information security officer, as well as the absence of the components for a good security program, also exposes the city to the risk of service disruption, and the potential release of private and sensitive information about city residents and employees should unauthorized parties hack into the city systems, breach existing controls, and steal sensitive information collected by the city during the course of performing its governmental functions. The cost of the hacks and breaches could cost the city millions in expenses related to credit reports, identity theft protections, and other requirements mandated by federal laws and regulations.

Recommendations

The Managing Director should direct DIT to:

10. Clarify authority and lines of responsibility for citywide security management by appropriately revising key planning documents and policies, administrative directives, and working with the mayor and city agencies to resolve coordination, management, and oversight issues;
11. Review current remediation practices and processes to determine which could be accomplished more effectively using automated versus manual processes, and review notification processes for non-security personnel when remediation is needed; and
12. Create an executive level position (Chief Information Security Officer - CISO) in DIT responsible for strategic and tactical information security initiatives, expand the role of security in DIT, require coordination among city departments for cybersecurity, and support the new function with additional information security and technical security personnel.

Chapter 4

Conclusions and Recommendations

The city's increasing reliance on information technology (IT) to support government services requires the city's IT security programs to be effective. Security policies and procedures must meet operational and security objectives, and cybersecurity operations should remediate IT security weaknesses. User security awareness and IT-security related personnel policies must support IT security; and responses to IT security incidents must be effective to protect city data, processes, and systems. Prior audits, consultant reports, and external financial information system audits of city security controls have itemized many deficiencies and made many recommendations for improving city security for its information systems.

Despite implementing many recommendations and greatly improving its IT technical security posture, we found the city is still vulnerable to unauthorized access to its data, resources, and information systems because it has not addressed typical IT security management concerns. The city and its Department of Information Technology (DIT) need to follow up on identified threats; improve communications within DIT and among city departments; and need to assess and validate security risks. City departments and DIT need to update security control policies and procedures; provide security awareness training; test incident response plans; and provide security information system staff authorization to implement security measures commensurate with their responsibilities. Without these improvements, the city remains highly vulnerable to disruption of services, unauthorized hacks, and system breaches that could cost the city millions in credit reports, identity theft protection, and other costs related to the unauthorized access to city information systems.

Recommendations

The Managing Director should direct DIT to:

1. Conduct periodic risk assessments of systems and applications to improve the organization's security posture and prevent incidents;
2. Create a citywide information user security awareness training that includes all users of information systems, external non-city users, and others who support the city's IT operations and assets;

3. Require security awareness training before anyone is permitted to access city information systems or applications, and include, but not be limited to, information security risks associated with users' activities; users' responsibilities in complying with city and department policies and procedures designed to reduce these risks; and training of personnel with significant responsibilities for information security;
4. Consider integrating information security concerns into human resources policies, particularly with respect to hiring, termination, and disclosure of sensitive information;
5. Improve access management by reducing reliance on manual methods and establishing timelines for department notifications to the DIT security administrator;
6. Review, assess, and implement cybersecurity controls that are appropriate and cost effective for immediate implementation and add value to security initiatives;
7. Regularly test incident response plans and develop an incident response program that plans, provides, modifies, and accommodates changes in the IT computing environment;
8. Develop and address PCI-DSS requirements before activating future plans for e-commerce and on-line transactions;
9. Update security control policies and procedures;
10. Clarify authority and lines of responsibility for citywide security management by appropriately revising key planning documents and policies, administrative directives, and working with the mayor and city agencies to resolve coordination, management, and oversight issues;
11. Review current remediation practices and processes to determine which could be accomplished more effectively using automated versus manual processes, and review notification processes for non-security personnel when remediation is needed; and
12. Create an executive level position (Chief Information Security Officer - CISO) in DIT responsible for strategic and tactical information security initiatives, expand the role of security in DIT, require coordination among city departments for cybersecurity, and support the new function with additional information security and technical security personnel.

Management Response

The Managing Director and the Department of Information Technology director agreed with 11 of the recommendations and implemented most of the recommendations in response to the draft reports. Due to lack of funding, management did not agree to create an executive position for cybersecurity (see Recommendation #12). The management comments were responsive to the audit recommendations. We made other technical, non-substantive changes to the draft report for purposes of accuracy, clarity, and style. A copy of management's full response can be found on page 52.

OFFICE OF THE MAYOR
CITY AND COUNTY OF HONOLULU

530 SOUTH KING STREET, ROOM 300 • HONOLULU, HAWAII 96813
PHONE: (808) 768-4141 • FAX: (808) 768-4242 • WEB: www.honolulu.gov



KIRK CALDWELL
MAYOR

ROY K. AMEMIYA, JR.
MANAGING DIRECTOR DESIGNATE
GEORGETTE T. DEEMER
DEPUTY MANAGING DIRECTOR

May 24, 2016

Mr. Edwin S. W. Young
Office of the City Auditor
City and County of Honolulu
1001 Kamokila Boulevard, Suite 216
Kapolei, Hawaii 96707

Dear Mr. Young:

SUBJECT: Audit of the City's Information Security and Risk Management Program

We are in receipt of your letter dated May 3, 2016, regarding the final draft report findings and recommendations of the *Audit of the City's Information Security and Risk Management Program*.

The Department of Information Technology (DIT) has provided the following responses to include comments, action plans, and anticipated dates of implementation to each of the recommendations.

Recommendations:

1. Conduct periodic risk assessments of systems and applications to improve the organization's security posture and prevent incidents;

Response: Agree. DIT will research and adopt a formalized risk assessment process based on an industry standard; pilot this process on one system; expand the risk assessment to systems that contain Personal Identifiable Information and confidential data; and perform risk assessments on all other systems.

Estimated implementation date: April 2017.

Mr. Edwin S. W. Young
May 24, 2016
Page 2

2. Create a citywide information user security awareness training that includes all users of information systems, external non-city users, and others who support the city's IT operations and assets;

Response: Agree. DIT will finalize the draft training plan that has been developed; acquire and pilot on-line training classes; expand on-line training to all users; and look at providing live training (Train the Trainer).

Estimated implementation date: September 2016.

3. Require security awareness training before anyone is permitted to access city information systems or applications, and include, but not be limited to, information security risks associated with users' activities; users' responsibilities in complying with city and department policies and procedures designed to reduce these risks; and training of personnel with significant responsibilities for information security;

Response: Agree. DIT is finalizing the draft training plan that has been developed; develop specific new employee training material; conduct Train the Trainer classes (security liaisons/Computer Services Representatives); and have the trainers train new employees.

Estimated implementation date: July 2016.

4. Consider integrating information security concerns into human resources policies, particularly with respect to hiring, termination, and disclosure of sensitive information;

Response: Agree. This is one of DIT's ongoing processes. DIT has implemented automatic syncing of information between Human Resources (HR) and Active Directory; implemented a process to automatically disable users based on HR inactive status; is in the process of developing a system to automatically re-enable users based on HR active status for contract workers; and is exploring the feasibility of automatically creating an Active Directory user based on the HR on-boarding process.

Estimated implementation date: Ongoing.

5. Improve access management by reducing reliance on manual methods and establishing timelines for department notifications to the DIT security administrator;

Mr. Edwin S. W. Young
May 24, 2016
Page 3

Response: Agree. DIT will be developing an application to automate the attestation of global groups.

Estimated implementation date: December 2016.

6. Review, assess, and implement cybersecurity controls that are appropriate and cost effective for immediate implementation and add value to security initiatives;

Response: Agree. This is one of DIT's ongoing processes. DIT has implemented Kerberos for Single Sign-On, Secure Sockets Layer for establishing an encrypted web sessions and tighter control over user accounts and access.

Estimated implementation date: Ongoing.

7. Regularly test incident response plans and develop an incident response program that plans, provides, modifies, and accommodates changes in the IT computing environment;

Response: Agree. DIT will review and update the incident response plan and implement tabletop exercises to help test the plan.

Estimated implementation date: December 2016.

8. Develop and address PCI-DSS requirements before activating future plans for e-commerce and on-line transactions;

Response: Agree. DIT is in the process of engaging Cisco to perform a Payment Card Industry (PCI) Data Security Standard (DSS) Readiness Assessment.

Estimated implementation date: June 2016.

9. Update security control policies and procedures;

Response: Agree. DIT will update the Cybersecurity Plan, Security Policy, and the Cybersecurity Incident Response Plan.

Estimated implementation date: December 2016.

Mr. Edwin S. W. Young
May 24, 2016
Page 4

10. Clarify authority and lines of responsibility for citywide security management by appropriately revising key planning documents and policies, administrative directives, and working with the mayor and city agencies to resolve coordination, management, and oversight issues;

Response: Agree. DIT will update the Security Policies and Mayor's directive.

Estimated implementation date: December 2016.

11. Review current remediation practices and processes to determine which could be accomplished more effectively using automated versus manual processes, and review notification processes for non-security personnel when remediation is needed; and

Response: Agree. DIT will review and update the incident response plan.

Estimated implementation date: December 2016.

12. Create an executive level position (Chief Information Security Officer – CISO) in DIT responsible for strategic and tactical information security initiatives, expand the role of security in DIT, require coordination among city departments for cybersecurity, and support the new function with additional information security and technical security personnel.

Response: Security has always been one of the core functions of DIT. The nature of the security work may have evolved due to rapid changes in how the City utilizes the information technology resources. DIT appreciates the support of the City's Auditor Office in additional staffing; however, DIT does not have funding to create an executive position at this time.

The administration and DIT appreciate the fine work of the Office of the City Auditor, and we look forward to receiving and using the final audit report to further our efforts to improve the City's security and risk management system.

Warm regards,



Roy K. Amemiya, Jr.
Managing Director

This page intentionally left blank.

Appendix A

Audit Objectives, Scope and Methodology

Pursuant to Section 3-502.1(c) of the Revised Charter of Honolulu and the Office of the City Auditor's Annual Work Plan for FY2014-15, this audit was self-initiated. The audit objectives were to: (1) assess the state and effectiveness of the city's information technology security management program; (2) assess the implementation of effective user security awareness and information technology security related personnel policies to support IT security; and (3) assess the capability and effectiveness of the city's cybersecurity operations.

We reviewed applicable charter provisions, ordinances, laws, rules and regulations, departmental policies and procedures, annual reports, budgets, financial documents, plans, and other documentation related to the department's capabilities to fulfill its mission and purposes related to security controls and service continuity.

Our audit reviewed a selection of general IT security controls as applied and managed by the Department of Information Technology (DIT), including risk assessment, policies and procedures, security administration procedures for key systems, user awareness training, and cybersecurity and incident response plans.

The review covered legal requirements and internal policies, procedures, and verbal or written administrative guidance related to such controls and activities. We assessed the impact of these controls on operations and the ability to meet departmental and other relevant city security objectives.

Some autonomous agencies such as the Honolulu Police Department and the agencies of the City Council of Honolulu were reviewed in a limited way to assess and evaluate their contributory and consumer role in citywide information technology security.

The audit focused primarily on citywide IT security management, and general information controls applied over departmental systems, operations and resources. We reviewed security administration procedures and supplemental activities related to IT security objectives. We also reviewed and assessed the city's disaster cybersecurity and incident response plans, which are also managed by the department's security administration section.

The audit did not cover system level controls (e.g., network, operating system, or infrastructure applications), business process application controls, or controls applied by other departments over their facilities, resources or services. The audit did not include backup and recovery procedures implemented at any of the other city departments, or those applied to systems outside the control of the data center. The audit did not cover client/server recovery or other operational level maintenance related to recovering individual resources applied by the department. As the audit concerned general controls, activities of personnel, and management of security, we did not assess the reliability of computer systems themselves or computer-processed data. We did not test the adequacy or effectiveness of technical controls.

The audit reviewed the adequacy of the department's security framework to protect the city's critical information systems and data by comparing it to commonly used industry security

standards. The standards included relevant controls, data management, and service continuity. We conducted visual observation and reviews of operations at the department's data center and the security administration section, focusing on their operational activities, security roles and responsibilities, and related activities.

We reviewed the high level management role in coordinating and integrating the current applied information security framework. We also reviewed previous assessments of departmental information security to determine whether the department addressed previously identified issues and problems. We conducted interviews with department management, security administration supervisor and staff, and other departmental staff whose primary function relates to the administration of security controls to determine past and current practices. We also interviewed selected personnel from other agencies related to the department's management of security policy, roles, and coordination.

We researched and reviewed selected internet, literature, and technology information resources to identify commonly utilized information security and cybersecurity frameworks, controls and practices used by government and industry. We researched the National Institute of Standards and Technology (NIST), the Council on Critical Security Controls, InfoSec Security Institute, and federal information system management controls for security management and practices.

The prior Office of the City Auditor's Audit of Selected City Information Technology Controls (Report N. 06-01, January 2006) reported the Department of Information Technology did not provide sufficient oversight and planning to protect and secure key city information technology resources and systems. The report stated the department control framework, physical and environmental controls, and disaster recovery planning were inadequate. Financial audits from FY 2010 to FY 2014 identified shortcomings in city information system general controls such as passwords, change management, and access to city information resources and systems.

The audit was performed in accordance with generally accepted government auditing standards from November 2014 to April 2016. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B

Glossary of Terms and Definitions

Active Directory Synchronization (ADSync) typically refers to integration applications that focus on synchronizing and reconciling active directory entities to its system infrastructure. Its primary use is to forward active directory user updates to their system environment and provide a “same login” experience to users.

Integrated Identity Management is the use of information technology to manage individual user identities, their authentication, authorization and privileges within or across the system. The privileges are within the enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.

Kerberos, version 5 is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. It is designed so that a client can prove its identity to a server (and vice versa) across an insecure network connection, and their communications can be encrypted to assure privacy and data integrity.

Lightweight Directory Access Protocol (LDAP) is open, vendor-neutral, industry standard application/protocol for accessing and maintaining distributed information services over an Internet Protocol (IP) network.

Multi-Protocol Label Switching (MPLS) is a network data-carrying technique that promotes efficient routing. Applications can include traffic engineering and implementing virtual private networks. Using this technique can result in lower cost, extended scalability, improved reliability, and increased security of network data.

Public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically between a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

Single sign-on (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications.

This page intentionally left blank.

Appendix C

Risk Assessment

The National Institute of Standards and Technology (NIST) Standards' *Risk Management Guide for Information Technology Systems* lists nine steps for assessing information system security risks:

1. Define the scope of the risk assessment, characterize the IT system, and identify system boundaries, resources, and information that constitute the system;
2. Identify and document potential threat sources; identify any circumstance or event with the potential cause; and identify the intentional or unintentional harm to an IT system;
3. Develop a list of technical and non-technical system flaws or weaknesses (vulnerabilities) that could be exploited or triggered by the potential threat sources;
4. Document and assess the effectiveness of technical and non-technical controls implemented or to be implemented that minimize or eliminate the likelihood of a threat exploiting a vulnerability;
5. Determine the likelihood or probability that a vulnerability could be exploited by a threat source given the existing or planned security controls;
6. Determine the level and adverse impact from a threat exploiting a vulnerability (considering the organization's mission; the value or importance of the affected system or data; the associated costs; and the loss of confidentiality, integrity, or availability of the systems and data);
7. Determine the risk level that represents the degree or level of risk that an IT system, facility, or procedure might be exposed to if a given vulnerability were exploited;
8. Identify controls that could reduce or eliminate the identified risks to the organization's operations; and
9. Document the risk assessment results in an official report or briefing to senior management that makes decisions on policy, procedure, budget, system operations and management changes.

This page intentionally left blank.

Appendix D

Future PCI Assessment Considerations

The Payment Card Industry Data Security Standards (PCI-DSS), Requirements and Security Assessment Standards, version 3.1, were issued and effective in April 2015. Under a full PCI compliance assessment, standard 12.10 contains several assessment requirements related to implementing an incident response plan and responding immediately to a system breach. More specifically:

- PCI DSS 12.10.2 requires that an incident response plan should be tested annually. The standard indicates that without proper testing, key plan steps may be missed, which could result in increased exposure during an incident. DIT has not tested its current response plan, but will need to annually test the plan to be PCI compliant.
- PCI standard 12.10.4 requires appropriate training of security staff responsible for responding to security breaches. The standards also require designated and specific personnel to be available on a 24/7 basis to respond to alerts. Currently, the city's incident response plan would not satisfy PCI standard 12.10.4 assessment criteria. In the city plan, the incident response team is formed on an ad hoc basis, team members are not pre-trained for their planned roles and responsibilities, and the DIT security administrator is tasked to identify DIT staff and train them to perform the selected incident response functions. Our assessment confirmed their response was reactive and did not focus on the need of staff to practice, test, and become familiar with their planned roles so that they responded to incidents as quickly and effectively as possible if they became incident response team members. This is an important aspect of incident response readiness. As a result, DIT and the city currently cannot ensure sufficient personnel are trained and will be available on a 24/7 basis to respond to alerts and prevent extended damage to the city network, critical data, and city systems.
- PCI standard 12.10.6 indicates there should be a process to modify and evolve the incident response plan according to the lessons learned and the changes should incorporate current security developments. Since DIT has not tested its plan, the city cannot improve or identify changes needed in its plan, and currently would not pass this assessment criteria.

This page intentionally left blank.

Appendix E

Presidio Risk Assessment and Recommendations for Top Ten Critical Findings – City and County of Honolulu (2009)

<i>Critical Issue</i>	<i>DIT Implementation of Recommendations</i>
No information security strategy	Create an information security organization with an executive level position responsible for strategic and tactical information security initiatives. Recommendations not implemented.
Significant number of systems missing critical software patches	Recommendations implemented.
Significant number of hardware/software systems no longer supported by vendor	Recommendations implemented.
No network segmentation at the wide area network or local area network	Recommendations implemented.
No internal network security controls	Recommendations implemented.
No centralized monitoring solution in place	Recommendations implemented.
No information security monitoring	Recommendations implemented.
Lack of comprehensive application security solution	Recommendations implemented.
Sensitive data on mobile computers	Recommendations not implemented.
Mobile computer left open connected to City network	Recommendations not implemented.

Note: The Department of Information Technology technical implementation of the security recommendations and the consultant's recommendations of technical implementations were omitted for security reasons. The status, Recommendations not implemented, does not mean no security measures are in place.

Source: Presidio Networked Solutions, City and County of Honolulu Risk Assessment, May 27, 2009, Office of the City Auditor

This page intentionally left blank.

Appendix F

Critical Security Controls

No.	Critical Security Controls	Department of Information Technology (DIT) Implementation
1.	<p>Inventory of Authorized and Unauthorized Devices</p> <p><i>Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. (CSC, pp. 8-13)</i></p>	DIT has implemented controls in this area.
2.	<p>Inventory of Authorized and Unauthorized Software</p> <p><i>Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. (CSC, pp. 14-18)</i></p>	DIT has implemented controls in this area.
3.	<p>Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers</p> <p><i>Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. (CSC, pp. 19-26)</i></p>	DIT has implemented controls in this area.
4.	<p>Continuous Vulnerability Assessment and Remediation</p> <p><i>Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. (CSC, pp. 27-32)</i></p>	DIT has implemented controls in this area.
5.	<p>Malware Defenses</p> <p><i>Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. (CSC, pp. 33-37)</i></p>	DIT has implemented controls in this area.
6.	<p>Application Software Security</p> <p><i>Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. (CSC, pp. 38-42)</i></p>	DIT has implemented controls in this area.
7.	<p>Wireless Access Control</p> <p><i>The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANs), access points, and wireless client systems. (CSC, pp. 43-47)</i></p>	DIT has implemented controls in this area.

No.	Critical Security Controls	Department of Information Technology (DIT) Implementation
8.	<p>Data Recovery Capability</p> <p><i>The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it. (CSC, pp. 48-50)</i></p>	DIT has implemented controls in this area.
9.	<p>Security Skills Assessment and Appropriate Training to Fill Gaps</p> <p><i>For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs. (CSC, pp. 51-53)</i></p>	DIT has implemented controls in this area.
10.	<p>Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</p> <p><i>Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. (CSC, pp. 54-57)</i></p>	DIT has implemented controls in this area.
11.	<p>Limitation and Control of Network Ports, Protocols, and Services</p> <p><i>Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. (CSC, pp. 58-61)</i></p>	DIT has implemented controls in this area.
12.	<p>Controlled Use of Administrative Privileges</p> <p><i>The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. (CSC, pp. 62-67)</i></p>	DIT has implemented controls in this area.
13.	<p>Boundary Defense</p> <p><i>Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. (CSC, 68-74)</i></p>	DIT has implemented controls in this area.

No.	Critical Security Controls	<i>Department of Information Technology (DIT) Implementation</i>
14.	<p>Maintenance, Monitoring, and Analysis of Audit Logs</p> <p><i>Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. (CSC, 75-79)</i></p>	DIT has implemented controls in this area.
15.	<p>Controlled Access Based on the Need to Know</p> <p><i>The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. (CSC, pp. 80-83)</i></p>	DIT has implemented controls in this area.
16.	<p>Account Monitoring and Control</p> <p><i>Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them. (CSC, pp. 84-88)</i></p>	DIT has implemented controls in this area.
17.	<p>Data Protection</p> <p><i>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. (CSC, pp. 89-94)</i></p>	DIT has implemented controls in this area.

No.	Critical Security Controls	Department of Information Technology (DIT) Implementation
18.	<p>Incident Response and Management</p> <p><i>Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems. (CSC, pp. 95-97)</i></p>	DIT has implemented controls in this area.
19.	<p>Secure Network Engineering</p> <p><i>Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers. (CSC, pp. 98-100)</i></p>	DIT has implemented controls in this area.
20.	<p>Penetration Tests and Red Team Exercises</p> <p><i>Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker. (CSC, pp. 101-104)</i></p>	DIT has implemented controls in this area.

Source: Council on Cyber Security. The Critical Security Controls for Effective Cyber Defense, Version 5.0 (CSC) and Office of the City Auditor.

Appendix G

Critical Elements for Security Management
















No.	<i>Critical Elements for Security Management</i>	<i>Current Department of Information Technology (DIT) Implementation</i>
1	Establish a security management program	<p>DIT applies a citywide, centralized technical security administrative function, and manages IT security for the city except for the semi-autonomous Board of Water Supply.</p> <p>It currently is not a well-defined IT security management program which has policies, plans, and procedures that clearly describe and define the entity's security management program, its activities, objectives and performance measures. The performance of the program in other security management elements is listed in the following rows.</p> <p>Previous audits and reviews have identified the lack of an executive level IT security officer as a contributing cause of the city not developing elements of well-rounded security management program, which may diminish the city's overall IT security posture and potentially result in unknown risks and vulnerabilities.</p>
2	Periodically assess and validate risks	<p>DIT currently does not do formal, documented risk assessments as part of its operations or to define its IT security management program activities and operations.</p> <p>As needed prior to implementations, DIT reports considering the technological risks of implementing new technology, and related practical technical security concerns of the implementation.</p>
3	Document and implement security control policies and procedures	<p>The current set of policies and plans are outdated, and may not be applicable to the current security and technological environment.</p> <p>DIT reports that it applies technical security controls to address the resulting threats.</p>
4	Implement effective security awareness and other security-related personnel policies	<p>There is no current user security awareness training to ensure safe and secure use, and limited IT security-related personnel policies. DIT issues a periodic newsletter to provide topical security awareness information to city users. Employees are initially given IT security policies at orientation, and must acknowledge them prior to using the city's email and Internet.</p> <p>In response to the draft report, DIT has developed a plan in March 2016 to implement a comprehensive Security Awareness and Training program, which will monitor and evaluate effectiveness of awareness and training efforts, and update the program on an ongoing basis.</p>

No.	<i>Critical Elements for Security Management</i>	<i>Current Department of Information Technology (DIT) Implementation</i>
5	Monitor the effectiveness of the security program	<p>DIT employs technical measures and reports internally concerning the technical effectiveness of its security program.</p> <p>An important aspect to this monitoring is to ensure that policies and plans intended to reduce risk are effective on an ongoing basis, which is a test of general IT security effectiveness that is currently not well-developed in the department.</p> <p>This aspect stands in addition to effective technical monitoring and tests of IT controls to evaluate or determine whether they are appropriately designed and operating effectively to meet control objectives.</p>
6	Effectively remediate information security weaknesses	<p>Current posture of DIT security administration is reactive. The security administration section currently uses a mix of automated and manual processes to identify and remediate security problems. Remediation, coordination, and notification issues with current security administration processes were noted during audit fieldwork.</p> <p>Depending on the IT data, system, or process involved, DIT needs to comply with state and federal laws, and follow industry guidelines (e.g., Social Security, PCI, HIPAA, Act 10, and CJIS).</p>
7	Ensure that activities performed by external third parties are adequately secure	DIT conducts reviews over third party access, and provides access management controls over third party usage.

Source: GAO Federal Security Controls Audit Manual (2009) and Office of the City Auditor

Appendix H

Survey Questions and Results From Departments Regarding Information Technology Systems and Security Policies^a

Survey Questions	Survey Results	Comments
Has the department developed its own IT policies (e.g. user policies, IT security policy, Internet policy)?	Yes  5 No  12	DIT and city IT policies state that city departments have the responsibility to develop their own IT security policies that are consistent with and supplement DIT's security policies and guidelines. However, most city departments surveyed have not, and rely solely on DIT to provide adequate security for their critical IT systems and network. Therefore, DIT and city IT security policies and guidelines are ineffective because they do not promote departmental IT security policymaking.
Has the department identified and assessed IT security threats to its critical systems and data, and determined ways to eliminate or control these threats by developing an IT internal risk assessment?	Yes  6 No  11	DIT and city IT policies state that city departments have the responsibility to develop a departmental technology risk assessment to review and identify its critical IT systems for disaster preparedness, and in the event that information or computer programs are destroyed, improperly altered, or stolen. Most city departments surveyed have not developed their own risk assessments. Therefore, DIT and city IT security policies are ineffective to assess risks facing the citywide and internal departmental IT programs.
Does the department have a business continuity plan to ensure operational business functions and data protection in the event of an IT infrastructure outage or security event?	Yes  9 No  8	Standards state computer security incidents may undermine the business resilience of the organization, and business continuity planning should consider security incidents and their impacts. However, DIT has never tested recovery from a cyber security incident. Without testing, DIT is unable to discover deficiencies in its planned incident response, and can't determine if the plan is adequate or relevant to current threats.
Are users trained before operating computers and other IT equipment within the department?	Yes  13 No  4	Most city departments train their employees to use IT equipment that they will use to perform their job, but the city lacks user awareness training or security personnel training needed to support and maintain a viable security program.
Does the department maintain a list of users and their level of access to the systems and data?	Yes  13 No  4	Most city departments maintain a list of users and their level of access, but former city employees, contractors, and non-users are able to access city systems because their accounts weren't terminated in a timely manner by DIT.
Does the department have policies on protecting and handling data containing personal information?	Yes  13 No  4	Sensitive information is not protected using data loss prevention to prevent export of sensitive data by end-users. In our opinion, sensitive information wasn't protected appropriately because this security control was not implemented by DIT.
Has the department ever experienced downtime, loss of productivity, or an inability to service the public due to security threats such as unauthorized users or malware?	Yes  3 No  14	The surveyed departments reported four security incidents resulting in downtime, loss of productivity, and an inability to service the public due to security threats like unauthorized use or malware. One department had an incident with Cryptowall ransomware, which although detected by DIT, the lack of notification and remediation resulted in a loss of user productivity, two months of work, and permanently inaccessible files. Two incidences concerning malware via email were reported. Also, a department's confidential files may have been exposed for months on the Internet due to setting improper security settings for the city's document management system.
Has the department ever received assistance from DIT in identifying, classifying, and securing its data or the creation of IT security policies?	Yes  12 No  5	Most city departments rely on DIT to provide security over their IT systems and resources. However, DIT lacks sufficient authority to implement a citywide security program, and only provides technical support. The lack of data classification, security, and policymaking support may make its technical security efforts ineffective or inappropriate for departmental needs.

^a Survey Results from 17 city departments and agencies.

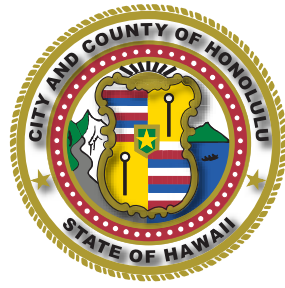
Source: Office of the City Auditor Survey Results

This page intentionally left blank.

Appendix I

Technology Roadmap

This page intentionally left blank.



Technology Roadmap

City and County of Honolulu

Department of Information Technology

April 2016

