Department of Controlled Substances (DCS) IT Narrative

*For IT Security and Audit Seminar, Case Study*

*Authors: Matt Robinett, CISA, MSIS, COBIT & Charles Ross, CISA, CISM, MSIS*

# High Level Back Ground:

The Department of Controlled Substances (DCS), is an agency under the legislative branch of the state government. This agency governs the wholesale purchase, distribution, and retail sales process of all controlled substances under the Controlled Substances Act (CSA). The CSA is regulated to the Joint Legislative Action and Resolution Committee (JLARC), made up of twelve state assembly men/women. A four-person board, appointed by the governor, provides oversight and leadership to DCS. The board serves a tenure of four years. No two staff members exit their tenure in the same year. The executive staff (C-Suite) provide day-to-day operations leadership.

DCS contains a small internal law-enforcement unit with deputized officers, given the ability to investigate controlled substance-related crimes and are able to detain, question, and arrest suspected criminals. DCS agents are required to abide by all law enforcement codes of conduct and applicable laws that apply to all other state and local police and sheriff’s officers.

DCS has 349 employees, with a variety of departments: robust in-house Information Technology arm, administrative functions, business management, marketing, statistics/analytics division, legal team, and procurement department.

**Financial Overview:**

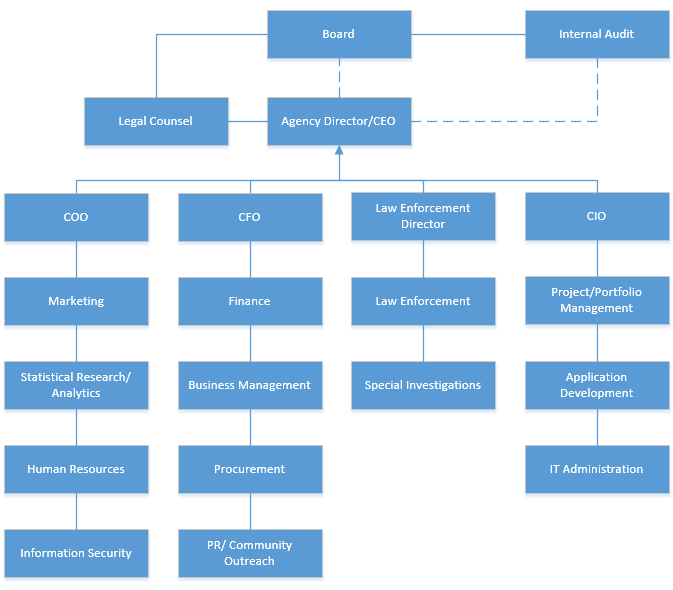
|  |  |
| --- | --- |
| Total 2013 Budgeted Revenue | $30,450,375 |
| General Revenue Fund | $13,450,375 |
| Special Revenue Fund | $17,000,000 |
| Actual 2013 Revenue | $30,684,922 |
| Payroll | $6,589,412 |
| Expenditures | $11,945,367 |

**Governing References and Standards:**

Internal Policies and Procedures

Commonwealth IT Security Standard SEC501-09

# Organizational Diagram:



# IT Narrative Overview:

**DCS Network:**

DCS is segmented into three main network segments: the Administrative System, the Public Relations System, and the Consumer/Sales System. While there are other systems that are used, these three comprise the overwhelming majority of all relevant operations for the business.

Administrative System (Sensitivity Level: **VERY HIGH- FINANCIAL, PII, HIPAA**):

The Administrative System is responsible for managing all administrative aspects of the business group. This includes HR, Financial, Financial Reporting, Payroll, etc. This system is broken down into two sub-systems: the Human Resources (HRMS) and Financial Reporting (FRMS) management systems. These systems are responsible for providing administrative support to the business. These systems are classified as sensitive with respective to internal financial and payroll data, employee personal identifiable information (PII), medical data regulated by HIPAA (drug-tests are performed as a condition of hiring for all employees, which is classified as medical information), and other applicable data that is associated with HR and Finance systems.

All software aspects (database, middleware, and application tiers) of the Administrative System are owned, controlled, and managed by DCS with in-house developers, administrators, and managers. However, the infrastructure components are not physically located in-house. See “Infrastructure Management” for more information about system management.

Consumer/Sales System (Sensitivity Level: **VERY HIGH- FINANCIAL, PII, PCI**):

The Consumer/Sales System is responsible for managing all aspects of the sales and inventory aspects of DCS. This includes Sales and Revenue, Point-of-Sale transactional data, PCI (credit card) data, inventory management, and merchandise procurement. This system is comprised of two sub-systems: The Warehouse Inventory Management (WIMS) and Point-of-Sale (POS) Systems. These systems are responsible for moving and managing inventory from business satellite stores (WIMS) and for accepting payments, processing and recording transactions (POS). The POS System transmits reconciliations, sales, taxes, etc. to the FRMS in order to properly calculate revenue, expenditures, sales, and other relevant financial information, which is used in DCS’s financial reporting process.

Like the Administrative System, all software aspects (database, middleware, and application tiers) are owned, controlled, and managed by DCS with in-house developers, administrators, and managers. However, the infrastructure components are not physically located in-house. See “Infrastructure Management” for more information about system management.

Public Relations System (Sensitivity Level: **MODERATE - INTERNAL MARKETING INFO**):

The Public Relations (PR) System is responsible for managing all aspects of the public outreach and marketing of issues involving the responsible use of legal controlled substances and advocacy for reducing the use of illegal controlled substances. This function involves marketing paraphernalia, school outreach, community services, and research analytics.

DCS partners with a marketing firm, Drugs-Are-Bad-Mkay, LLC (DABM), to perform all applicable research, analytics, trend analysis, design PR campaigns, and develop academic and community outreach programs. DCS does not house any system components of the PR System in-house, nor does DCS own any system components. Instead, DCS receives quarterly reporting on market research from DABM from a dedicated VPN (AES-256 bit encryption), of which the reports do not contain any sensitive information. Furthermore, DCS uses this same dedicated VPN to upload marketing plans and strategies, which DABM uses to develop their outreach programs. The most recent SOC-2 report (September 2015) revealed no material weaknesses or control deficiencies.

The PR System contains marketing and research information that, while not sensitive to the organization, is mission-critical for the operations of public relations operations. While information is considered to be internally sensitive, a data breach would not necessarily be damaging to the company and no legal ramifications would occur. Known risks only come from compromising data integrity or availability.

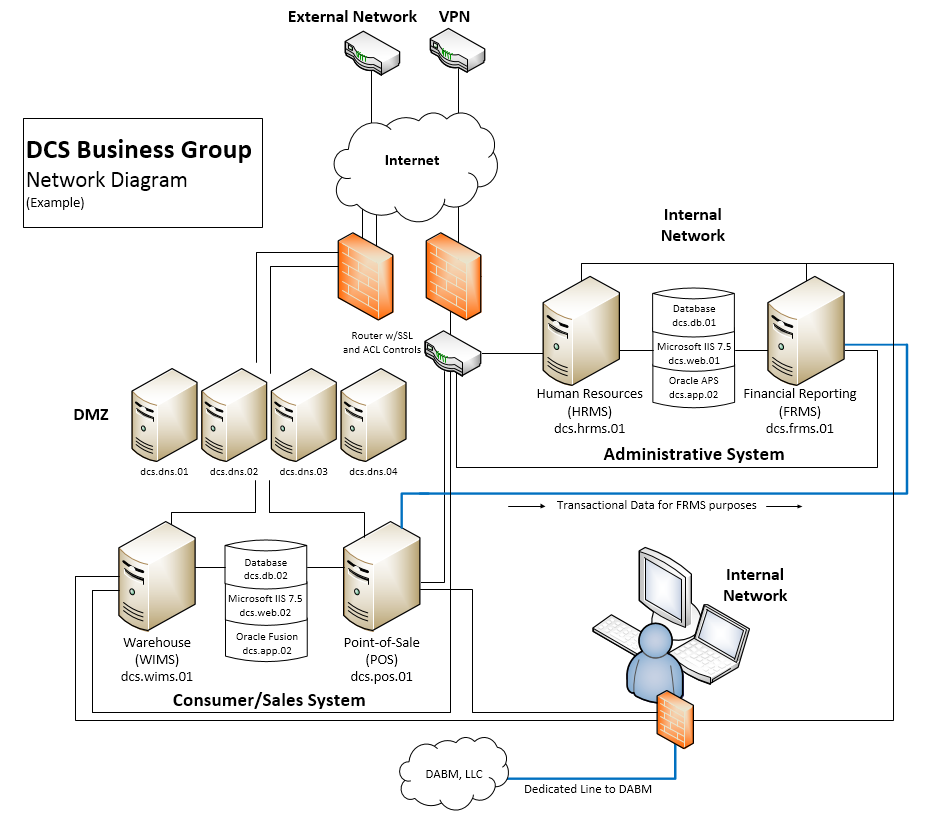
**Network Access:**

DCS employees have two methods of accessing the network. They may access the network from the onsite machines and workstations that are connected via wired Ethernet in-office or access the network through a segmented VPN that utilizes AES 128-bit encryption (outdated standard) and requires a username/password combination and Key FOB plugged into their agency-supplied machine (two-factor authentication).

There are three firewalls- one protecting the VPN access to the internal network, one delegated specifically for DABM data collection/dissemination, and one for the external network access that is used by vendors, the public, and contractors. The external access firewall is a singular gateway for many sources of contact and remains the most critical of firewalls on the network.

There is an external network that is available to vendors and retail stores that require access to ordering forms through the WIMS application. The WIMS application for supply orders is on the dcs.wims.01 server (see server listings below) and allows customers, vendors, and employees to access supply levels, inventory orders, pending orders, and shipping status for existing orders. This access is controlled via LDAP methodology (for external customers) and active directory (for internal customers/employees with accounts).

**Network Diagram:**



**Sensitive and/or Critical Systems:**

|  |  |
| --- | --- |
| Human Resource Management System (HRMS) | Point-of-Sale System (POS) |
| Financial Reporting Management System (FRMS) | Virtual Private Network (VPN) |
| Warehouse Inventory Management System (WIMS) | ECMS (Change Management) |

**Infrastructure Management:**

DCS maintains all server and physical infrastructure components with a Third Party Administrator, “Peak Data Centers” (referred to, in this Narrative, as “Peak”). As such, no data centers or data hubs exist onsite at DCS, except for workstations and networking equipment.

Through a Service Level Agreement (SLA), Peak provides hosting services for Operating Systems and subsequent OS servers that support databases, applications, and middleware for the Administrative and Consumer/Sales Systems. This also includes any applicable IT Systems/Data Backup and Restoration requirements.

While Peak provides physical infrastructure hosting and managing services, it does not manage the software and related application servers. This includes database software, middleware, and presentation-layer applications. Additionally, Peak does not provide networking services, except what is used to secure their data centers (this is out of scope for DCS). These items are managed exclusively by DCS and are only affected by Peak management when a request is needed to modify the system files that support the software or applications. This is performed through a formal, documented change management process that is managed in-house by DCS (see “Change Management” sub-section below).

DCS’s contractual agreement with Peak requires Peak to manage a total of 12 servers at the operating system level, including database, application, web, and middleware servers. The listing below shows a snapshot of the server totals, the managing entity over these servers. DCS is responsible for managing a total of 12 system components at the application and database layers. Peak manages a total of 8 Operating Systems that run on Red-Hat Linux and support applications, databases, and middleware. Peak also manages 4 DNS Web Servers that support web-facing infrastructure for the applications.

DCS maintains Peak’s Service Organization Controls (SOC) Type 2 Report for the period under audit, July 1, 2014 – June 30, 2015, performed by a credible independent auditing firm, Deloitte & Touché, LLP.

Management has developed a formalized process for requesting, reviewing, and analyzing the bi-annual SOC-2 reports that are produced by Peak. Additionally, Peak includes specific controls to be audited every year as part of the Service-Level Agreement (SLA) with DCS. According to the most recent SOC-2 report, which was produced on September 15th, 2015, no control deficiencies or material weaknesses have been noted. As such, the SOC-2 report can reasonably be relied upon for adequate general controls coverage for the areas noted in the report. Soc-2 complimentary controls that have been identified are: logical access controls IT Security Awareness and Training, and Change Management.

|  |  |  |
| --- | --- | --- |
| **Coding Name** | **System/Application Supported** | **Responsible Party** |
| dcs.db.01 | Administrative Oracle DBMS | DCS |
| dcs.db.02 | Consumer/Sales Oracle DBMS | DCS |
| dcs.hrms.01 | HRMS Application Module | DCS |
| dcs.frms.01 | FRMS Application Module | DCS |
| dcs.pos.01 | Checkout 8.2 POS Application | DCS |
| dcs.wims.01 | Warehouse Inventory Mgmt App | DCS |
| dcs.web.01 | Microsoft IIS 7.5 for PeopleSoft | DCS |
| dcs.web.02 | Microsoft IIS 7.5 for PeopleSoft | DCS |
| dcs.app.01 | Oracle APS for Oracle Financials | DCS |
| dcs.app.02 | Oracle Fusion for Oracle Financials | DCS |
| Offsite | Administrative Server OS | Peak 12 |
| Offsite | Consumer/Sales Server OS | Peak 12 |
| Offsite | HRMS Application Server OS | Peak 12 |
| Offsite | FRMS Application Server OS | Peak 12 |
| Offsite | Administrative Oracle Server OS | Peak 12 |
| Offsite | Consumer/Sales Oracle Server OS | Peak 12 |
| Offsite | IIS Middleware Server OS | Peak 12 |
| Offsite | Oracle APS/Fusion App Server OS | Peak 12 |
| dcs.dns.01 | DNS Server | Peak 12 |
| dcs.dns.02 | DNS Server | Peak 12 |
| dcs.dns.03 | DNS Server | Peak 12 |
| dcs.dns.04 | DNS Server | Peak 12 |

**Software and Applications:**

DCS’s main software and application components are Oracle 11G R2 DBMSs and PeopleSoft Enterprise Resource Planning (ERP) software. The PeopleSoft ERP provides the modular functions for performing all tasks associated with the HRMS and FRMS systems and is supported by applicable Oracle DBMS instances. Integration is supported by several functional middleware and webserver components, which include Oracle Application Suite 12, Oracle Fusion Middleware 12G, and Microsoft IIS 7.5 webserver software. PeopleSoft, as a Commercial-Off-The-Shelf (COTS) product, was developed by Oracle, but is actively managed through a combination of DCS administrators and Oracle service-level agreements.

Additionally, warehouse management is delegated through a Warehouse Inventory Management Application (WIMA). WIMA was custom-built in 2004 by DCS developers and is managed in-house by DCS administrators. WIMA is a publically-facing web application that is built on the .NET Framework and, due to legacy-application restrictions, must interface with an Oracle 9G DBMS and Oracle 9i middleware.

Point-of-Sale applications are in an application bundle accessible through retail outlet registers and designated workstations in the application Checkout 8.2 POS. It is a COTS product that passively managed by DCS developers/administrators. All changes made to the application are done through service-level agreements with the Checkout vendor through support calls and contractor fulfillment. A SOC-2 report is on file and reviewed bi-annually. No material weaknesses or control deficiencies were discovered in the SOC-2 reports as of the last SOC issuance date (July 2015). In review of the SOC report, no referenced complimentary controls were apparent.

**Security Awareness & Training:**

In a recent review from DCS’s Security Awareness and Training vendor, only 40% of employees have taken their required (by policy) annual IT Security Awareness and Training sessions. During further review, it was determined that no sincere effort is made to enforce training mandates, for new hires, existing employees, and IT System Administrator’s or Database Administrators.

**Mobile Device and Wireless Security:**

DCS began implementing a standardized mobile device methodology for accessing some sensitive information through an external network. As of 6/1/2015, the only resource that employees can currently connect to is an Exchange Email Server. You also determine that DCS does utilize a wireless network. After further investigation, the related wireless network is only an extension of DCS’s wired network and not providing any additional security over sensitive data.

**Change Management:**

DCS uses an enterprise-wide change management application called Enterprise Change Management System (ECMS). The ECMS has been developed and continues to be managed in-house by DCS employees. All functionality and business rules within the application are required to abide by standardized DCS change control governance policies. The system was developed in 2003 and has not undergone any significant changes since its inception.

DCS has developed an enterprise-wide change control governance policy that was reviewed in 2013. This policy was found to be antiquated and out of compliance with industry best-practices for change control. It is required, by policy, to be reviewed annually by the ECMS Council that is comprised of the CEO, COO, CIO, Audit Director (non-voting), Director of Applications, Director of Infrastructure & Support Services, and the Chief Information Security Officer (ISO). The council meets quarterly and develops policy updates when necessary. The last council review was in 2012.

**IT Systems/Data Backup and Restoration:**

Because Peak only supplies physical space to house infrastructure and day-to-day management of operating systems, DCS is responsible for the timely backup and restoration of their systems. In the 2014 audit, an Observation was written noting that no backup/restoration policy exists (violation of CP-9-COV) for their sensitive systems. In response to this Observation, DCS has developed an IT backup/restoration policy and has tested it in April 2015.

**Contingency and Risk Management:**

DCS has recently developed a new IT Disaster Recovery Plan and plans to test it in December of 2015. Likewise, policy requires that IT Risk Assessments must be updated every three years, or when environmentally necessary (SEC501, Section 6.2). The last IT Risk Assessments performed were in 2012. An audit review was performed in 2012 and found no material weaknesses or control deficiencies.

IT Systems and Data Classification is considered to not be part of the IT Risk Assessment process, but provides essential data to allow an organization to accurately develop their IT Risk Assessments. The last IT Systems/Data Classification review occurred in 2010.