INFORMATION SYSTEMS SECURITY PROGRAM

Department of Controlled Substances
FYE December 31st, 2015

This audit program covers the security over the information systems of the Department of Controlled Substances (DCS). A description of critical agency systems, security controls, and information system structure is documented in the following narrative. These systems support the processes described in the other audit programs comprising this entire audit project.

The test procedures in this program support the systems security test objectives well as the audit objectives outlined in the program. However, it does not test all internal controls built into information systems used by the Department of Controlled Substances (DCS). System controls that provide for things such as data accuracy and completeness (application controls) should be addressed in the appropriate business process audit program.

Step 1: Narrative

Provide the detailed narrative of the Agency's or Institution's IT Environment as it relates to the audit objectives and financial assertions of the general audit program. Document the internal control processes as they relate to the confidentiality, integrity, and availability of information.

Step Completed by & Date: [Insert Name & Date]
Step Reviewed by & Date: [Insert Name & Date]

CONTACTS

Chuck Ross	Chief Information Officer
rosscd@vcu.edu	804.XXX.XXXX
Matt Robinett	Chief Information Security Officer
robinettmw@vcu.edu	804.XXX.XXXX

NARRATIVE

The IT Narrative can be found embedded in the attached document, labeled "DCS IT Narrative.docx".

DCS IT Narrative(2)
(1).docx

Step 2: Scope

Document the scope limitations for this particular project. Be as specific as possible when describing particular systems. Please list specific system names, platforms, and the applications they support. Also, document the reasoning for the scope of this particular program. Include how compensating controls will be evaluated in the absence of documented policies and procedures, or whether a management point is warranted.

In my opinion, based on the agency's procedures described above and an evaluation of their internal control structure, the audit procedures listed below are adequate.

Group sign/date: [Group 4, 04/05/2017]
Project Manager sign/date: [Matt will sign off, and Date]

SCOPE

1. DCS has recently developed a new IT Disaster Recovery Plan and planned to test it in December 2015. To ensure the test went through, we would need to retest and audit the Disaster Recovery plan to make sure that the procedures and steps for restoring IT systems after a disaster are up-to-date and effective. Having a proper Disaster Recovery plan provides a sense of security, minimizes risks of delays, guarantees the reliability of standby systems and decision making during a disaster. Not having a proper Disaster Recovery Plan could lead to loss in revenue because it could halt business processes.

2. The WIMS is responsible for moving and managing inventory from all the satellite stores. It is hosted on the dcs.wims.01 server. This application holds several data ranging from medium to high sensitivity. Because the WIMS holds confidential records, like Financial Information and Personal Identification Information, not properly conducting the Risk Assessment and securing this type of information could lead to user distrust and ruin DCS's reputation.

Program Legend: *** Stay away from bright colors, please! ***
Joanna Senseng
Mouhanad Azzam
Reem Kuwaifi
Yonis Ainab
Mohammed Khoori

AUDIT PROCEDURES

Step 3: Planning

A. Document the discussions and meeting that took place to derive your scope. Include class sessions with instructors, emails/conversations directly with instructors and your cohorts, industry research, and risks you noted in the DCS IT Narrative.

B. Prepare the *DCS Case Study* Excel document and embed it in the planning section.

Step Completed by & Date: [Insert Name & Date]
Step Reviewed by & Date: [Insert Name & Date]

Auditor Planning Documentation

Group Four met on 3/29/2017 during class time to discuss potential scope choices we plan to audit. During this meeting, Group 4 were assigned the scopes, Disaster Recovery Plan and the IT Risk Assessment of the Warehouse Inventory Management System, to audit. On 4/5/2017, Group 4 conversed with the instructor on areas where the DRP and WIMS can be improved and revised, such as reviewing dates for documents, checking if certain processes that needed to be implemented exist, and verifying if certain requirements are included. On 4/6/2017, Group 4 discussed our thoughts over email and came to the conclusion that the WIMS Risk Assessment and the Disaster Recovery Plan play an important role in the IT environment of the DCS because we want to minimize loss of revenue from unforeseeable disasters and negate from becoming a disreputable company if sensitive data gets released. Later that day, Group 4 met up to discuss what risks these two scopes can hold for the company. We decided that the Disaster Recovery Plan needed to be audited to ensure that the steps of restoring data after a disaster are up to date and effective. We believed it was necessary to audit, because if the plan was flawed it could lead to loss in revenue for the company. The WIMS is also necessary to be audited, because the system is in charge of managing and moving inventory from the businesses satellite store. We believed it could impose risks for the company in that if it were not properly secured hackers could easily access the system.

Step 4: Preliminary Risk Assessment

Considering the audit risk, fraud risk, internal controls, determine and document the following risks and the supporting information for the system security process:

*Control risk is the risk that an error could occur in an audit area, and which could be material, individually or in combination with other errors, but the internal control system will not prevent or detect and correct the error on a timely basis.

Step Completed by & Date: [Insert Name & Date]
Step Reviewed by & Date: [Insert Name & Date]

PRELIMINARY RISK ASSESSMENT

Based on the preliminary review of DCS, Group 4 determined that the control risk is high for the IT Risk Assessment for WIMS, due to the fact that it is responsible for managing all aspects of the sale and inventory for DCS. The critical area will be handling the personnels who are responsible for managing the data. They have access to sensitive data and they need to make sure that the data is not lost. For the IT Disaster Recovery Plan we determined that the control risk is also high, due to the fact that it is a procedure that protects DCS's infrastructure and sensitive data in the event of a disaster. The current Disaster Recovery Plan has not been properly tested or ensured it works correctly which can pose many threats.

TEST WORK

While the Confidentiality, Integrity, and Availability of information relating to financial statements are maximized through a mature Information Security Program and the concept of "defense-in-depth", that is, there is an exponential relationship between the layers of information security controls in place to the level of protection achieved; the audit test work in this program is focused and based on the identified risks above.

Step 5: [IT Risk Assessment(WIMS)]

Contacts (Name, Title, and Contact info):

Chuck Ross rosscd@vcu.edu	Chief Information Officer 804.XXX.XXXX
Matt Robinett robinettmw@vcu.edu	Chief Information Security Officer 804.XXX.XXXX
Step Completed by & Date:	[Insert Name & Date]
Step Reviewed by & Date:	[Insert Name & Date]

Conclusion: After reviewing the IT RISK Assessment (WIMS) Group 4 determined that it is not reasonable. By comparing Risk Assessment for the WIMS with Business Impact Analysis, we determined that the information from each document is inconsistent with each other. Because the BIA is a comprehensive review of the impact of the risks included in the RA, it would be inaccurate if the information is misconstrued from one document to another.

DEEMED NOT REASONABLE

Step 1: (Policy Existence)

		Yes	No	N/A
A.	Does the Agency have a documented Risk Assessment?	X		

Step 2: (Policy Completeness)

Obtain and review the RA for the WIMS and determine whether:

A. The IT System information documented in the BIA is consistent with the RA. Specifically consider the following elements of each artifact:
   a. System Sensitivity Classifications
   b. Data Type Classifications
   c. Data Sensitivity Classifications

After reviewing documents “DCS IT Risk Assessment (WIMS).doc” and “DCS Business Impact Analysis.xlsx” for WIMS, Auditor Senseng, Auditor Azzam, and Auditor Kuwaifi, noted that the levels of sensitivity are inconsistent on both documents. For the System Sensitivity Classification, the WIMS RA noted that it does not process sensitive data. The BIA, however, states that WIMS does contain sensitive data, and ranks it at a low impact. For the Data Type Classifications, the WIMS RA noted that it handles both Financial Information and Personal Identification Information. Under “Column O” of the BIA, it lists only the following : Inventory, Sales Data, PCI, Vendor Records, Expenditures, which does not include any information in relation to PII.

DEEMED UNREASONABLE

B. Vulnerabilities, threats, safeguards, threat probabilities, loss impacts, and recommendations are documented.

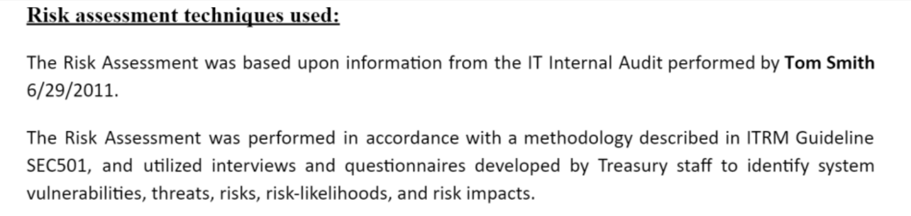
Auditor Kuwaifi reviewed the document, “DCS IT Risks Assessment (WIMS),” and noted that it does not include vulnerabilities, safeguards, loss impacts, and recommendations.

DEEMED UNREASONABLE

C. A process exists to conduct an annual self-assessment to determine the continued validity of the RA and updated if warranted.

Auditor Azzam noted on page 2 of DCS IT Risks Assessment (WIMS) that a process exists for conducting an annual self-assessment to determine the continued validity of the RA.
Tom Smith, Internal Audit Director, conducted the IT Internal Audit on the 29th of June 2011 with the methodology outlined in the ITRM Guideline SEC501. The RA was last updated on on 5/20/2012. It stated that it should be reviewed and updated annually.

Source:



Risk assessment techniques used:

The Risk Assessment was based upon information from the IT Internal Audit performed by **Tom Smith** 6/29/2011.

The Risk Assessment was performed in accordance with a methodology described in ITRM Guideline SEC501, and utilized interviews and questionnaires developed by Treasury staff to identify system vulnerabilities, threats, risks, risk-likelihoods, and risk impacts.

Page 2 of DCS IT Risks Assessment (WIMS).doc

DEEMED UNREASONABLE

D. A process exists to prepare an annual report that minimally includes:

1) identification of all vulnerabilities discovered during the self-assessment
2) an executive summary of the major findings and risk mitigation recommendations.

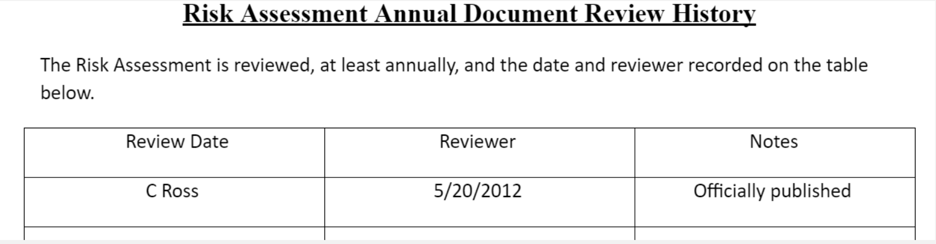
Auditor Kuwaifi reviewed the “DCS IT Risks Assessment (WIMS).doc” and noted that there was no identification of vulnerabilities or an executive summary of the major findings on it. We contacted the Chief Information Security Officer requesting this information. He later informed us that the company currently has no process for preparing an annual report.

DEEMED UNREASONABLE

Step 3: (Procedural & Control Implementation)

A. Determine whether the RA has been updated within the last 3 years or earlier if warranted.

Auditor Senseng reviewed the “DCS IT Risk Assessment (WIMS),” and it only contains one entry, which was completed by C Ross on 5/20/2012. Policy indicates that the RA needs to be reviewed at least annually.



Risk Assessment Annual Document Review History

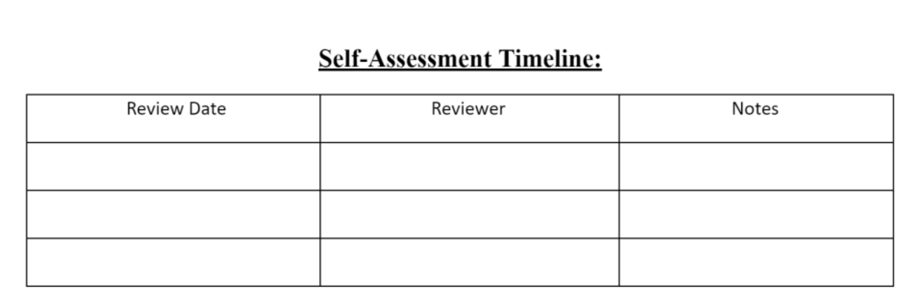
The Risk Assessment is reviewed, at least annually, and the date and reviewer recorded on the table below.

Review Date	Reviewer	Notes
C Ross	5/20/2012	Officially published

DEEMED UNREASONABLE

B. Determine whether an annual self-assessment has been conducted to determine the continued validity of the RA.

Auditor Ainab reviewed “DCS IT Risk Assessment (WIMS).doc” and noted that there are no entries indicating that an annual self-assessment has been conducted.



Self-Assessment Timeline:

Review Date	Reviewer	Notes

DEEMED UNREASONABLE

C. Determine whether a report has been prepared that minimally includes: identification of all vulnerabilities discovered during the self-assessment and an executive summary of the major findings and risk mitigation recommendations.

Auditor Azzam reviewed “DCS IT Risk Assessment (WIMS).doc” and determined that a report including the identification of all vulnerabilities discovered during the the self-assessment and an executive summary of the major findings and and risk mitigation recommendations was not included.

DEEMED UNREASONABLE

Step 6: Disaster Recovery Plan

Contacts (Name, Title, and Contact info):

Chuck Ross	Chief Information Officer
rosscd@vcu.edu	804.XXX.XXXX
Matt Robinett	Chief Information Security Officer
robinettmw@vcu.edu	804.XXX.XXXX
Step Completed by & Date:	[Insert Name & Date]
Step Reviewed by & Date:	[Insert Name & Date]

Conclusion: Auditor Kuwaifi, Auditor Azzam, and Auditor Senseng determined the Disaster Recovery Plan to be inconsistent. We noted the DRP is not consistent in the fact that it has not been approved by the agency head. A signature from the CEO is required in order to note that the DRP has been reviewed and approved. The DRP does state that an annual review is required, but it is not consistent in the fact that there is no documentation of any testing. The DRP is also not consistent in the fact that although the recovery requirements are listed, the vendor contacts are not. After contacting the Chief Information Security Officer, we noted that the current DRP has not yet been properly tested. We

determined this to not be reasonable, because it does not comply with the Commonwealth's Standard of requiring testing of the disaster recovery plan.

DEEMED NOT REASONABLE

Step 1: (Policy Existence)

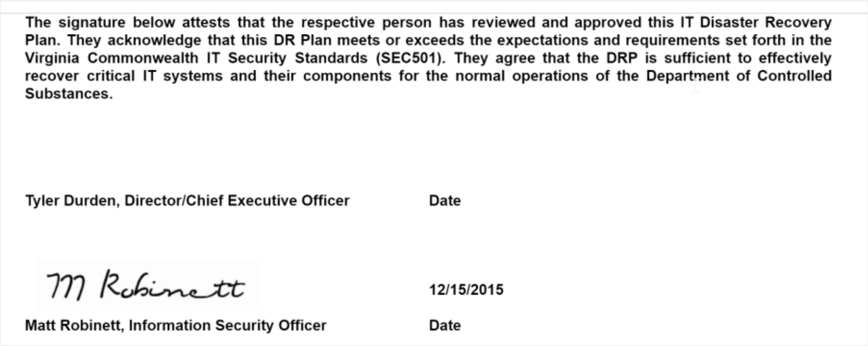
		Yes	No	N/A
A.	Does the Agency have a documented Disaster Recovery Plan?	X		

Step 2: (Policy Completeness)

Obtain and review the Agency's DRP and determine whether:

A. The DRP has been approved by the Agency Head.

Auditor Senseng reviewed "DCS IT Disaster Recovery Plan.doc" and noted that the Director/CEO, Tyler Durden, did not sign to attest that he has reviewed and approved this IT Disaster Recovery Plan. A signature is needed to approve the DRP.



The signature below attests that the respective person has reviewed and approved this IT Disaster Recovery Plan. They acknowledge that this DR Plan meets or exceeds the expectations and requirements set forth in the Virginia Commonwealth IT Security Standards (SEC501). They agree that the DRP is sufficient to effectively recover critical IT systems and their components for the normal operations of the Department of Controlled Substances.

Tyler Durden, Director/Chief Executive Officer Date

M Robinett 12/15/2015

Matt Robinett, Information Security Officer Date

DEEMED UNREASONABLE

B. Requirements are included to periodically review, reassess, test and revise to reflect changes in essential business functions, services, system hardware and software and personnel.

Auditor Kuwaifi reviewed the document "DCS IT Disaster Recovery Plan.doc" and noted that on pages 6-18, it documented the proper requirements of testing for the plan

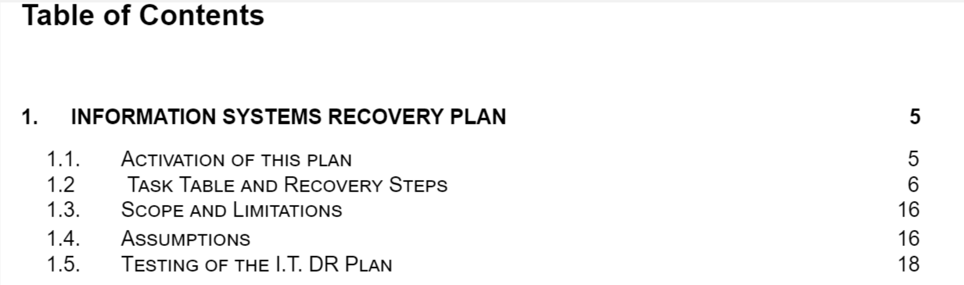
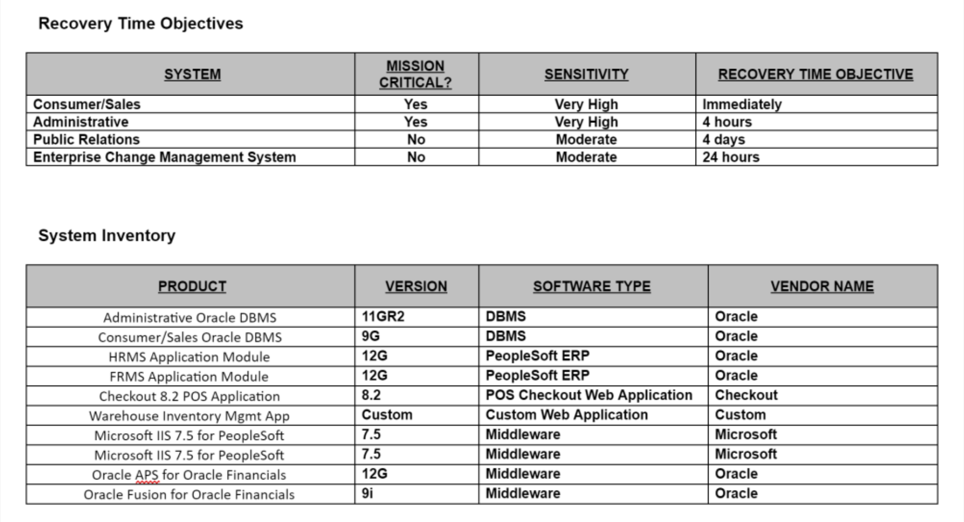


Table of Contents

DEEMED REASONABLE

C. The recovery requirements are identified for IT systems and data needed to support the essential business functions (based on BIA and RA), including system configurations, a list of hardware and software, and vendor contacts.

Auditor Khoori reviewed "DCS IT Disaster Recovery Plan.doc" and noted the list of hardware and software are documented on pages 23 and 24 and that the names of the vendors are also included.

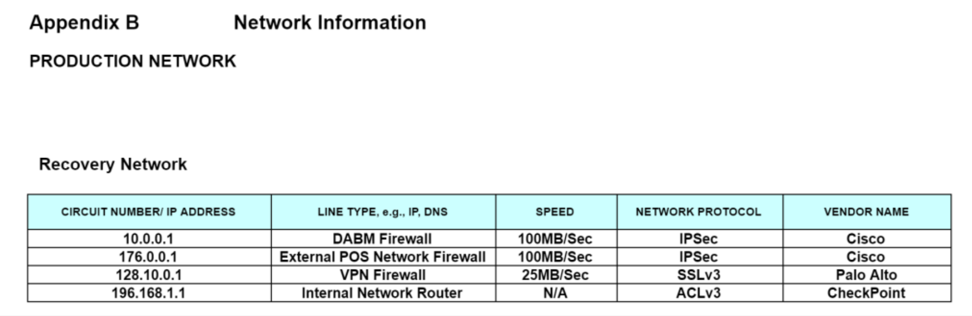


Recovery Time Objectives

SYSTEM	MISSION CRITICAL?	SENSITIVITY	RECOVERY TIME OBJECTIVE
Consumer/Sales	Yes	Very High	Immediately
Administrative	Yes	Very High	4 hours
Public Relations	No	Moderate	4 days
Enterprise Change Management System	No	Moderate	24 hours

System Inventory

PRODUCT	VERSION	SOFTWARE TYPE	VENDOR NAME
Administrative Oracle DBMS	11GR2	DBMS	Oracle
Consumer/Sales Oracle DBMS	9G	DBMS	Oracle
HRMS Application Module	12G	PeopleSoft ERP	Oracle
FRMS Application Module	12G	PeopleSoft ERP	Oracle
Checkout 8.2 POS Application	8.2	POS Checkout Web Application	Checkout
Warehouse Inventory Mgmt App	Custom	Custom Web Application	Custom
Microsoft IIS 7.5 for PeopleSoft	7.5	Middleware	Microsoft
Microsoft IIS 7.5 for PeopleSoft	7.5	Middleware	Microsoft
Oracle APS for Oracle Financials	12G	Middleware	Oracle
Oracle Fusion for Oracle Financials	9i	Middleware	Oracle



Appendix B Network Information

PRODUCTION NETWORK

Recovery Network

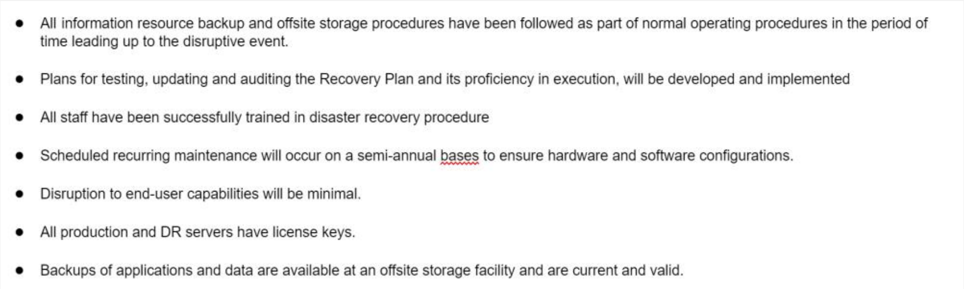
CIRCUIT NUMBER/ IP ADDRESS	LINE TYPE, e.g., IP, DNS	SPEED	NETWORK PROTOCOL	VENDOR NAME
10.0.0.1	DABM Firewall	100MB/Sec	IPSec	Cisco
176.0.0.1	External POS Network Firewall	100MB/Sec	IPSec	Cisco
128.10.0.1	VPN Firewall	25MB/Sec	SSLv3	Palo Alto
196.168.1.1	Internal Network Router	N/A	ACLv3	CheckPoint

DEEMED REASONABLE

Step 3: (Procedural & Control Implementation)

A. A copy of the DRP is stored in a designated plan repository (hard copy should be stored at accessible, secure off-site location).

Auditor Kuwaifi reviewed “DCS IT Disaster Recovery Plan.doc” and noted that the DCS IT DR Plan has been developed under assumptions. One of the assumptions included that a copy of the DRP is available offsite and are current and valid.



- All information resource backup and offsite storage procedures have been followed as part of normal operating procedures in the period of time leading up to the disruptive event.
- Plans for testing, updating and auditing the Recovery Plan and its proficiency in execution, will be developed and implemented
- All staff have been successfully trained in disaster recovery procedure
- Scheduled recurring maintenance will occur on a semi-annual bases to ensure hardware and software configurations.
- Disruption to end-user capabilities will be minimal.
- All production and DR servers have license keys.
- Backups of applications and data are available at an offsite storage facility and are current and valid.

DEEMED REASONABLE

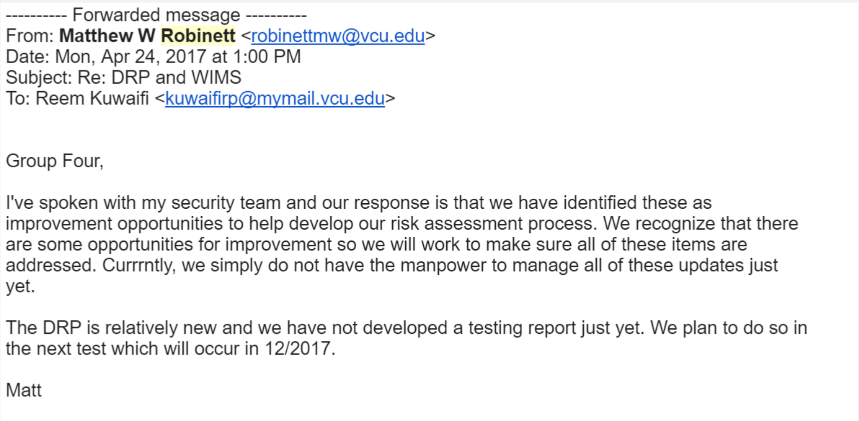
B. Determine whether the Agency periodically reviews, reassess, tests and revises the DRP to reflect changes in essential business functions, services, system hardware and software and personnel.

Auditor Kuwaifi reviewed “DCS IT Disaster Recovery Plan.doc” and noted that the documentation of testing the DRP was not included. After contacting the Chief Information Security Officer of the company, it was determined that the DRP is new. It is stated that it is mandatory to annually test the DRP.

DEEMED UNREASONABLE

C. The DRP is tested annually (i.e., recovery from backup tapes). Review documentation showing date of test, what was tested, results, and recommendations.

Auditor Azzam reviewed “DCS IT Disaster Recovery Plan.doc” and noted that in section 1.5, it states that an annual test is mandatory. Since the DRP is new and has yet to be tested, we cannot verify formal reviews of the DRP because there hasn’t been an opportunity to do that. A DRP test is scheduled to be conducted in 12/2017.



---------- Forwarded message ----------
From: **Matthew W Robinett** <robinettmw@vcu.edu>
Date: Mon, Apr 24, 2017 at 1:00 PM
Subject: Re: DRP and WIMS
To: Reem Kuwaifi <kuwaifirp@mymail.vcu.edu>

Group Four,

I've spoken with my security team and our response is that we have identified these as improvement opportunities to help develop our risk assessment process. We recognize that there are some opportunities for improvement so we will work to make sure all of these items are addressed. Currrntly, we simply do not have the manpower to manage all of these updates just yet.

The DRP is relatively new and we have not developed a testing report just yet. We plan to do so in the next test which will occur in 12/2017.

Matt

DEEMED UNREASONABLE

WRAP-UP

Step 7: Observations

A. Develop observations for management letter comments and project manager. Communicate impact of audit findings on the auditor's' testwork. Document the results.

B. Obtain and document management response to management points. Document final assessment of management point to determine if point is written (in report) or verbal.

C. Include a write up of the controls in place and/or any weaknesses (findings) in a format that can be used for the next years audit planning meeting.

Step Completed by & Date: [Insert Name & Date]
Step Reviewed by & Date: [Insert Name & Date]

MANAGEMENT POINTS

Auditor developed a total of 6 potential management recommendations:

OBS#	PY MP Title	Step #
1	Risk Assessment	7
2	Disaster Recovery Plan	8

Auditor communicated potential observations to Matt Robinett, DCS Information Security Officer on May 3,2017.

Auditor officially provided DCS the observations on 5/3/2017. The Observations are embedded below:

NEWWIMS (1).docx drp obsv.docx

DCS provided a response to the recommendations on 5/7/2017.

Auditor noted that DCS did concur with the observations:
"DCS management responded to the observations listed in fieldwork, via email. In this response, DCS concurred with the observations and provided a corrective action plan that will be distributed internally amongst relevant parties. Plans to address these concerns should occur in 2018." - Matt Robinett, DCS Information Security Officer

Auditor determined that, based on Management's response, two observations will be included in the report.

Step 8: Final Risk Assessments

Perform final assessment of control risk. If control risk is changed then impact must be considered and documented.

Control risk is the risk that an error could occur in an audit area, and which could be material, individually or in combination with other errors, but the internal control system will not prevent or detect and correct the error on a timely basis.

Step Completed by & Date:	[Insert Name & Date]
Step Reviewed by & Date:	[Insert Name & Date]

FINAL RISK ASSESSMENT

*Auditor determined that the preliminary control risk is **high.***

The preliminary risk level for the Disaster Recovery Plan is high. We have come to this conclusion, because the DRP has not been formally approved by the Agency head, has not been properly tested, and there is no documentation showing that it has been reviewed and revised.

The preliminary risk level for WIMS Risk Assessment is high.We have come to this conclusion, because the Risk Assessment does not contain the system sensitivity, data type or data sensitivity classifications. It has also not been properly documented and updated. The Risk Assessment is also missing an executive summary on all the major findings and risk mitigation recommendations.

Step 9: Conclusion

Conclude to audit program objectives. All auditors completing testwork need to sign and date conclusion.

Group sign/date: [Audit Group Number “Group X”, and Date]
Project Manager sign/date: [Matt will sign off, and Date]

CONCLUSION

In our opinion, based on the audit work performed, the audit objectives 1 & 2, except for the weaknesses noted in Step 8, as listed in the scope narrative, have been met.