Deloitte.

State of South Carolina –
Information Security Analysis

Weekly Status Report

April 12, 2013

Table Content

Reporting Date: April 12, 2013

I. Executive Summary Dashboard

Reporting Date: April 12, 2013

	Timeline impacted, address ASAP		Timeline may be impacted		On schedule, no major issues		Project milestone not started

Accomplishments

Agency	Immediately Address Serious Security Vulnerabilities	Security Risk Assessments
B&CB	• Continued with Cyber Threat Intelligence (CTI) diagnostics review • Web application scanning on ORS completed and selected the applications for detailed analysis	• Completed information security domain preliminary interviews / workshops, and follow-up inquires. • In process of identifying gaps and drafting initial gaps and recommendations.
PPP	• External/Internal scanning completed and undergoing analysis • Started CTI diagnostics	• Completed information security domain preliminary interviews / workshops, and follow-up inquires. • In process of identifying gaps and drafting initial gaps and recommendations.
DHEC	• Internal scanning in progress • In process of conducting web application scanning • Continued log analysis process for CTI diagnostics • Completed the firewall review and analysis	• Completed information security domain preliminary interviews / workshops, and follow-up inquires. • In process of identifying gaps and drafting initial gaps and recommendations.

Risk/Issues

- No issues or risks identified

Highlights

- All Risk assessment follow up activities completed and analysis of gaps in process
- Governance sessions in process and interviews with CISO's of MN, PA, and MI have been completed.
- Web application testing for SCI and DSIT hosted web applications will be performed only after the third party consent letters are signed and approved.
- Conducted first executive steering team meeting

Status	Milestone	Start	End	%
	Kick off with each agency	3/25	3/27	100
	Immediately Address Serious Security Vulnerabilities	3/26	4/25	60
	Security Risk Assessments	3/26	4/25	60
	Strategy and Recommendations	3/26	5/01	40

II. Vulnerability Assessment – B&CB

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
🟢	🟢	🟡

Status Key:

Status	Definition
🟢	On schedule, no major issues
🟡	Timeline may be impacted
🔴	Timeline impacted, address ASAP
○	Project milestone not started

OVERALL (60%)

Accomplishments to Date

- Completed the scanning on the Internal IP addresses in scope and communicated key observations from the initial analysis.
- Web application scanning and analysis has been initiated and additional testing window was requested for selected applications (based on initial list of vulnerabilities) .
- Started with the log analysis for CTI diagnostics
- Completed firewall review analysis on two firewalls.
- Initiated the process to scan the SCI hosted applications

Activities Planned for the Upcoming Week

- Continue the scanning and analysis on the B&CB target network ranges and applications
- Log analysis for the diagnostics services
- Application scanning on B&CB (SCEIS and DSIT hosted applications) as per the schedule

Issues and Risks

- Agreement with SCI LLC for testing – in process

Decision Log

- The selection of the web applications and additional testing window was communicated
- The third party hosted applications (SC1) will not be tested until the third party consent letter is signed before week of April 15, 2013.

Status	Milestone	Start	End	%
🟢	Planning and Kick Off	3/23	3/26	100
🟢	External network vulnerability test	3/23	4/12	100
🟢	Internal network vulnerability test	3/26	4/15	90
🟡	Web application vulnerability testing	3/26	4/21	50
🟢	Intranet cyber compromise diagnostic	3/26	4/21	40
🟢	Remote access diagnostic	3/26	4/21	30
🟢	Rogue device discovery diagnostic	3/26	4/21	20
🟢	Firewall rule set/ACL analysis	3/26	4/14	70
🟢	Assess perimeter security monitoring	4/8	4/21	10
○	Reporting	3/23	4/24	0

Follow up Items

- SC1 Hosted Application testing consent letter

II. Vulnerability Assessment – DHEC

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
		

Status Key:

Status	Definition
	On schedule, no major issues
	Timeline may be impacted
	Timeline impacted, address ASAP
	Project milestone not started

OVERALL (60%)

Accomplishments to Date

- External vulnerability assessment and analysis is complete
- Completed the vulnerability scanning on the selected hundred systems
- Review of the firewall configurations is complete
- Started log analysis for CTI diagnostics
- Initiated with the web application scanning on the external sites

Activities Planned for the Upcoming Week

- Continue with the internal scanning and internal web application
- Continue with the CTI diagnostics on logs that are obtained

Issues and Risks

- None

Decision Log

- None

Status	Milestone	Start	End	%
	Planning and Kick Off	3/23	3/26	100
	External network vulnerability test	3/26	4/12	100
	Internal network vulnerability test	3/26	4/21	65
	Web application vulnerability testing	4/8	4/21	30
	Intranet cyber compromise diagnostic	3/26	4/21	40
	Remote access diagnostic	3/26	4/21	30
	Rogue device discovery diagnostic	3/26	4/21	20
	Firewall rule set/ACL analysis	3/26	4/14	90
	Assess perimeter security monitoring	4/8	4/21	10
	Reporting	3/23	4/24	0

Follow up Items

II. Vulnerability Assessment – PPP

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
🟢	🟢	🟢

Status Key:

Status	Definition
🟢	On schedule, no major issues
🟡	Timeline may be impacted
🔴	Timeline impacted, address ASAP
○	Project milestone not started

OVERALL (60%)

Accomplishments to Date

- Completed the initial vulnerability scanning on the internal hosts.
- Completed the external scans on the Internet ranges
- Discussion with the DSSIT team members (hosted environment for the PPP web site) is complete and documented the web scanning procedures for their consent on the scanning activities.
- Log analysis for CTI diagnostics has been started

Activities Planned for the Upcoming Week

- Continue with the log analysis for the CTI diagnostics
- Perform application testing on the identified internal applications

Issues and Risks

- None

Decision Log

- The third party hosted applications (DSIT) will not be tested until the third party consent letter is signed before week of April 15, 2013.

Status	Milestone	Start	End	%
🟢	Planning and Kick Off	3/23	3/26	100
🟢	External network vulnerability test	3/26	4/21	10
🟢	Internal network vulnerability test	3/26	4/21	45
○	Web application vulnerability testing	4/15	4/21	0
🟢	Intranet cyber compromise diagnostic	3/26	4/21	40
🟢	Remote access diagnostic	3/26	4/21	30
🟢	Rogue device discovery diagnostic	3/26	4/21	20
🟢	Firewall rule set/ACL analysis	3/26	4/14	70
🟢	Assess perimeter security monitoring	4/8	4/21	10
○	Reporting	3/23	4/24	0

Follow up Items

State of South Carolina Information Security Risk Assessment

III. Information Security Risk Assessment – B&CB

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
		

Status Key:

Status	Definition
	On schedule, no major issues
	Timeline may be impacted
	Timeline impacted, address ASAP
	Project milestone not started

OVERALL (60%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops, and follow-up inquires.
- Compiled internal assessment tool identifying risk, control activity, as well as drafting initial gaps and recommendations.

Activities Planned for the Upcoming Week

- Recommend and rationalize observations for reporting purposes based on the current state assessment.
- Conduct classification analysis for identified gaps.
- Create draft report and conduct internal review.

Issues and Risks

- None

Decision Log

Status	Milestone	Start	End	%
	Planning and Kick Off	3/23	3/26	100
	Understand security and privacy requirements	3/23	4/5	100
	Analyze the current state	3/26	4/12	75
	Recommend and rationalize	4/15	4/23	40
	Final report	4/15	4/24	10

Follow up Items

- None

III. Information Security Risk Assessment – DHEC

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
		

Status Key:

Status	Definition
	On schedule, no major issues
	Timeline may be impacted
	Timeline impacted, address ASAP
	Project milestone not started

OVERALL (65%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops, and follow-up inquires.
- Compiled internal assessment tool identifying risk, control activity, as well as drafting initial gaps and recommendations.

Activities Planned for the Upcoming Week

- Recommend and rationalize observations for reporting purposes based on the current state assessment.
- Conduct classification analysis for identified gaps.
- Create draft report and conduct internal review.

Issues and Risks

- None

Decision Log

Status	Milestone	Start	End	%
	Planning and Kick Off	3/23	3/26	100
	Understand security and privacy requirements	3/23	4/5	100
	Analyze the current state	3/26	4/12	85
	Recommend and rationalize	4/15	4/23	40
	Final report	4/15	4/24	10

Follow up Items

- None

III. Information Security Risk Assessment – PPP

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
		

Status Key:

Status	Definition
	On schedule, no major issues
	Timeline may be impacted
	Timeline impacted, address ASAP
	Project milestone not started

OVERALL (60%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops, and follow-up inquires.
- Compiled internal assessment tool identifying risk, control activity, as well as drafting initial gaps and recommendations.

Activities Planned for the Upcoming Week

- Recommend and rationalize observations for reporting purposes based on the current state assessment.
- Conduct classification analysis for identified gaps.
- Create draft report and conduct internal review.

Issues and Risks

- None

Decision Log

Status	Milestone	Start	End	%
	Planning and Kick Off	3/23	3/26	100
	Understand security and privacy requirements	3/23	4/5	100
	Analyze the current state	3/26	4/12	75
	Recommend and rationalize	4/15	4/23	40
	Final report	4/15	4/24	10

Follow up Items

- None

IV. Strategy and Recommendations

Reporting Date: April 12, 2013

Key Project Performance Indicators:

Scope	Schedule	Project Risks/Issues
		

Status Key:

Status	Definition
	On schedule, no major issues
	Timeline may be impacted
	Timeline impacted, address ASAP
	Project milestone not started

OVERALL (45%)

Accomplishments to Date

- Performed salary research and developed draft budget
- Continued discussion on key governance decisions
- Interviewed CISOs from Michigan, Pennsylvania, and Minnesota to further elaborate CISO governance recommendations
- Met with AT&T and DSIT to review two-factor authentication options

Activities Planned for the Upcoming Week

- Conduct follow-up meeting and finalize governance structure
- Finalize initial budget except a) Data encryption b) Two factor authentication which will be provided later
- Update draft of the governance recommendations

Issues and Risks

- None

Decision Log

- None

Status	Activity / Milestone	Start	End	%
	Strategy/recommendation analysis	4/1	4/26	65
	Develop Infosec Budget	4/1	4/26	30
	Develop CISO Governance Model	4/1	4/26	60
	Develop priority remediation recommendations	4/10	4/26	10
	Final Interim Executive Report	4/26	5/1	0

Follow up Items

- None