Deloitte.

State of South Carolina –
Information Security Analysis

Weekly Status Report

April 5, 2013

Table Content

Reporting Date: April 5, 2013

I. Executive Summary Dashboard

Reporting Date: April 5, 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	• External and internal scanning completed • Initiated the log collection process for Cyber Threat Intelligence (CTI) diagnostics • B&CB managed applications for analysis have been selected	• All workshops (3 of 3) completed • Follow up sessions in process • Documentation and data analysis in process
PPP	• External scanning scheduled • Internal scanning in progress • Initiated the log collection process for CTI diagnostics	• All workshops (3 of 3) completed • Follow up sessions in process • Documentation and data analysis in process
DHEC	• Internal scanning in progress • External scanning completed • Initiated the log collection process for CTI diagnostics	• All workshops (3 of 3) completed • Follow up sessions in process • Documentation and data analysis in process

Risk/Issues

- No issues or risks identified

Highlights

- All risk assessment workshops completed
- Web application testing has started and log collection process for CTI diagnostics in progress
- Initial governance sessions completed

Status	Milestone	Start	End	%
	Kick off with each agency	3/25	3/27	100
	Immediately Address Serious Security Vulnerabilities	3/26	4/25	40
	Security Risk Assessments	3/26	4/25	40
	Strategy and Recommendations	3/26	5/01	15

State of South Carolina Vulnerability Assessment

II. Vulnerability Assessment – B&CB

Reporting Date: April 05, 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 (40%)

Accomplishments to Date

- Analysis of vulnerabilities on B&CB network is complete (false positive analysis)
- Initiated the internal scanning on the Internal IP addresses in scope
- Application selection is completed and schedules for B&CB (ORS, SCEIS and DSIT) hosted applications are completed
- Log collection for diagnostics has been initiated and logs have been collected from different devices

Activities Planned for the Upcoming Week

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

Issues and Risks

- None

Decision Log

- The number of IP addresses and applications for vulnerability analysis has been agreed upon (Meeting date: April 3rd, 2013 with Jimmy and Lindsey).
- The third party hosted applications will not be tested until the third party consent letter is signed.

Status	Milestone	Start	End	%
	Planning and Kick Off	3/23	3/26	100
	External network vulnerability test	3/23	4/15	90
	Internal network vulnerability test	3/26	4/15	70
	Web application vulnerability testing	3/26	4/21	20
	Intranet cyber compromise diagnostic	3/26	4/21	15
	Remote access diagnostic	3/26	4/21	15
	Rogue device discovery diagnostic	3/26	4/21	15
	Firewall rule set/ACL analysis	3/26	4/14	25
	Assess perimeter security monitoring	4/8	4/21	0
	Reporting	3/23	4/24	0

Follow up Items

- Collect the remaining logs if required based on the CTI diagnostics results.

II. Vulnerability Assessment – DHEC

Reporting Date: April 05, 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 (30%)

Accomplishments to Date

- Analysis of vulnerabilities on DHEC external network is in progress (false positive analysis)
- Initiated the internal scanning on the Internal IP addresses in scope for DHEC
- Review of the firewall configurations has started on the primary internet firewall
- Log collection for CTI diagnostics has been initiated and logs are being collected from different devices

Activities Planned for the Upcoming Week

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

Issues and Risks

- Rogue device analysis will be based on the current list from Symantec anti-virus and windows patch systems.

Decision Log

- With the large number of IP addresses in scope for DHEC internal range, decision was made to select hundred (100) systems for vulnerability analysis
- The third party hosted applications will not be tested until the third party consent letter is signed.

Status	Milestone	Start	End	%
🟢	Planning and Kick Off	3/23	3/26	100
🟢	External network vulnerability test	3/26	4/21	90
🟢	Internal network vulnerability test	3/26	4/21	25
○	Web application vulnerability testing	4/8	4/21	0
🟢	Intranet cyber compromise diagnostic	3/26	4/21	10
🟢	Remote access diagnostic	3/26	4/21	10
🟢	Rogue device discovery diagnostic	3/26	4/21	10
🟢	Firewall rule set/ACL analysis	3/26	4/14	40
○	Assess perimeter security monitoring	4/8	4/21	0
○	Reporting	3/23	4/24	0

Follow up Items

- Need to confirm the internal applications hosted within DHEC (thick client or thin client) for the web application testing.

II. Vulnerability Assessment – PPP

Reporting Date: April 05, 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 (30%)

Accomplishments to Date

- Initiated the internal scanning on the internal IP addresses in scope for DHEC
- Review of the firewall configurations has started
- Access to the Security Information and Event Management (SIEM) solution was provided for log collection and diagnostics activities.
- Initiated the external scans on the internet ranges for PPP
- Initiated the discussion to identify the applications hosted internally (thick client and thin client)

Activities Planned for the Upcoming Week

- Continue with the internal scanning
- Continue with the CTI diagnostics on the received logs

Issues and Risks

- None

Decision Log

- The third party hosted applications will not be tested until the third party consent letter is signed.

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	4/8	4/21	0
🟢	Intranet cyber compromise diagnostic	3/26	4/21	10
🟢	Remote access diagnostic	3/26	4/21	10
🟢	Rogue device discovery diagnostic	3/26	4/21	10
🟢	Firewall rule set/ACL analysis	3/26	4/14	30
○	Assess perimeter security monitoring	4/8	4/21	0
○	Reporting	3/23	4/24	0

Follow up Items

- Need to confirm the internal applications hosted within DHEC (thick client or thin client) for the web application testing.

State of South Carolina Information Security Risk Assessment

III. Information Security Risk Assessment – B&CB

Reporting Date: April 5, 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 (40%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops
- Conducted follow up workshops for B&CB as needed

Activities Planned for the Upcoming Week

- Analyze the current state (ongoing); core team to be onsite full-time
- Review additional artifacts collected / observed during workshops
- Complete the assessment tool
- Conduct gap classification analysis and begin to populate draft report

Issues and Risks

- None

Decision Log

- None

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	50
	Recommend and rationalize	4/15	4/23	0
	Final report	4/15	4/24	0

Follow up Items

- Finalize / prepare risk assessment draft report template

III. Information Security Risk Assessment – DHEC

Reporting Date: April 5, 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 (40%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops
- Conducted follow up workshops for DHEC as needed

Activities Planned for the Upcoming Week

- Analyze the current state (ongoing); core team to be onsite full-time
- Review additional artifacts collected / observed during workshops
- Complete the assessment tool
- Conduct gap classification analysis and begin to populate draft report

Issues and Risks

- None

Decision Log

- None

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	50
	Recommend and rationalize	4/15	4/23	0
	Final report	4/15	4/24	0

Follow up Items

- Finalize / prepare risk assessment draft report template

III. Information Security Risk Assessment – PPP

Reporting Date: April 5, 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 (40%)

Accomplishments to Date

- Completed all information security domain preliminary interviews / workshops.
- Conducted follow up workshops for PPP as needed

Activities Planned for the Upcoming Week

- Analyze the current state (ongoing); core team to be onsite full-time
- Review additional artifacts collected / observed during workshops
- Complete the assessment tool
- Conduct gap classification analysis and begin to populate draft report

Issues and Risks

- None

Decision Log

- None

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	50
○	Recommend and rationalize	4/15	4/23	0
○	Final report	4/15	4/24	0

Follow up Items

- Finalize / prepare risk assessment draft report template

State of South Carolina Strategy and Recommendations

IV. Strategy and Recommendations

Reporting Date: April 5, 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 (15%)

Accomplishments to Date

- Developed PowerPoint report outline for governance discussions
- Reviewed Senate bill 334 fiscal impact statement and gathered input budget data
- April 3: Governance discussion completed
- April 4: Governance discussion completed

Activities Planned for the Upcoming Week

- April 10 and April 16 (date still to be finalized): continue governance discussion
- Develop a draft budget

Issues and Risks

- None

Decision Log

- None

Status	Milestone	Start	End	%
	Strategy/recommendation analysis	4/1	4/26	20
	Final Governance Report	4/26	5/1	0

Follow up Items

- None