State of South Carolina – Division of Information Security (DIS)

Information Security Policy Handbook – Appendices

Document Change History

Version Number	Release Date	Summary of Changes	Section No./ Paragraph No.	Changes Made By
1.0	22-Oct-2014	Handbook Appendices		

Table of Contents

1 Appendix A – Overview

Objective and Scope

Deloitte & Touche LLP ("D&T") provided assistance to the Division of Information Security ("DIS") in the form of guidance and training to State agencies on applying information security policies issued by DIS. The guidance and training was provided through three (3) different workstreams: policy workshops, pilot workshops and on-site visits designed with the common goal of providing an understanding of the thirteen (13) State information security policies and to facilitate and respond to agency questions, comments and challenges.

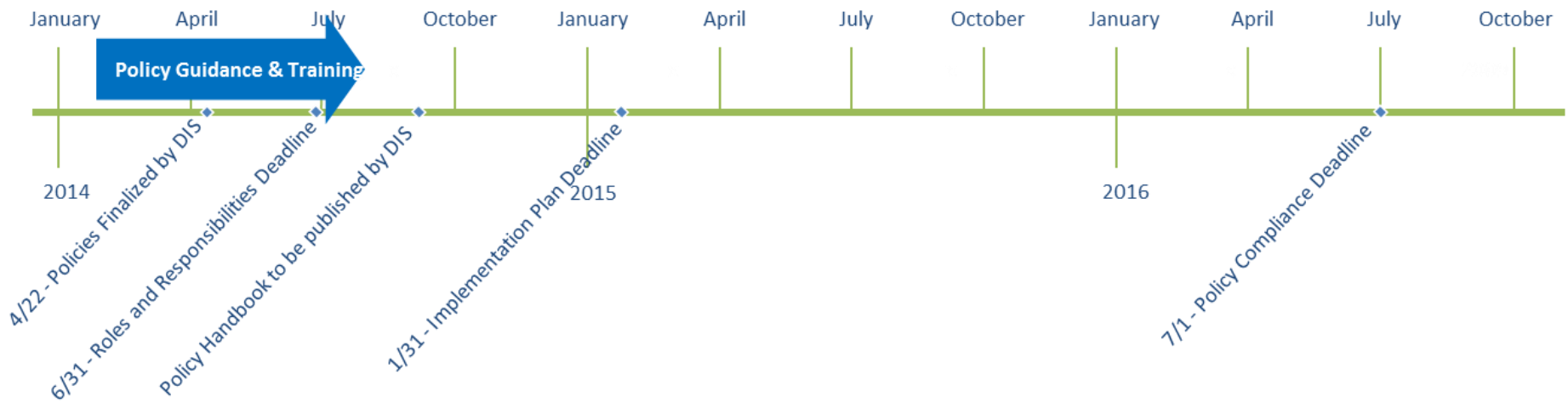
Information Security Policy Adoption Requirements

There are three (3) main dates/deadlines established by DIS to which agencies are expected to comply:

- ***June 30, 2014*** – ***Roles and Responsibilities*** – By this date, agencies were expected to have completed the 'Roles and Responsibilities Chart' (or equivalent template) posted on the DIS website. Havingie identified roles and responsibilities, an agency would have identified the individuals, teams, departments or third-parties that are needed to help complete gap analyses, implementation plans, training, coordination, etc., the components applicable for policy adoption. *For further details on the Roles and Responsibilities Chart template, please see section 3.2.*
- ***January 31, 2015*** **–** ***Implementation Plans*** – By this date, agencies need to complete and submit implementation plans that address all the gaps identified to DIS. An implementation plan should include details for how the agency plans to overcome their individual gaps with established timelines no later than the compliance date (see the next date below). *For further details on the Gap Analyses and Implementation Plan templates, please see section 3.2.*
- ***July 1, 2016*** **–** ***Compliance Date*** – By this date, agencies are expected to be compliant with all aspects of the State information security policies. Compliance in this respect means that agencies have addressed all gaps, implemented solutions and processes, have supporting documentation not only associated with the current procedures, but also for the security controls identified (e.g., user access reviews). In addition, agencies should have completed security awareness training associated with the State information security policies and training for new roles agency personnel might be responsible for maintaining the security posture.

The below is a high level timeline highlighting the deadlines and the important dates for the implementation of the statewide information security policies.

Figure 6. Policy Implementation Timeline



Templates Developed

As part of the policy guidance and training initiative, DIS developed a series of templates to help agencies navigate, understand and address their current situation and future strategies towards compliance with the new State policies. These materials are discussed in depth throughout the appendices on this document, including detailed examples and suggestions for how to use each template posted. The materials produced as part of this initiative are the following:

- ***Roles & Responsibilities Chart Template*** – This is designed to help agencies identify personnel who will be responsible for helping during gap analyses, brainstorm challenges, develop implementation strategies, approve policies, help with training and ultimately the implementation of new policies and procedures. This template was available to be leveraged to meet the June 30, 2014 DIS deadline for roles and responsibilities.
- ***Gap Analysis Templates*** – These are designed to aid agencies with identifying gaps against the State policies based on their current security environment. Each policy (13) is accompanied with an individual gap analyses template that simplifies each bullet or requirement from that policy in to slimed down, understandable series of questions.

- ***Implementation Plan of Action Template*** – This template accompanies the gap analysis templates and provides agencies with a suggested outline to document the strategies that are required for the agency to overcome each particular gap identified. Implementation plans are due January 31, 2015.

Key Activities

To help provide guidance and training to State agencies, the following individual workstreams were developed, approved and utilized over the course of the six (6) month initiative:

- ***Policy Workshops*** – Policy workshops of up to two (2) hours each, were conducted twice per month and broken down into groups of large, medium and small agencies with thirty (30) policy champions attending their respective session. During each policy workshop, agencies of similar size gathered together to receive guidance and discuss policies. Of the thirteen (13) State policies, ten (10) were selected for training based on level of complexity and risk:
    - *Asset Management*
    - *Data Protection & Privacy*
    - *Access Control*
    - *Information System Acquisition, Development & Maintenance*
    - *Threat & Vulnerability Management*
    - *Business Continuity Management*
    - *IT Risk Strategy*
    - *Mobile Security*
    - *HR & Security Awareness*
    - *Physical & Environmental Security*

Workshops start with a recap of the open questions from the previous session and the answer associated with that question which comes from DIS guidance. The majority of the meeting is then spent discussing the specific requirements or components from the particular policy, including pictorial representations of attributes, helpful guidelines and additional guidance that accompany the policy. Agencies also have the chance to collaborate and post open questions to the other policy champions in the room around implementation approaches or how a particular agency handled situations related to policy adoption. The

workshops also include overall risks, actual gaps identified from agency risk assessments (a separate workstream performing risk assessments for State agencies), as well as typical challenges found among agencies. Workshop presentations are uploaded to the DIS website for agencies to revisit and use at their disposal.

- ***Pilot Workshops*** – Three (3) pilot agencies were selected to represent the major group sizes of agencies; large, medium and small agency. For each of the selected agencies, assistance was provided for by conducting joint gap analyses, helping to fill out and review completed documentation and start building the foundation for implementation plans against the gaps identified. Over a series of seven (7) meetings lasting up to four (4) hours in length, D&T assisted and guided the pilot agencies through the below six (6) policies:
    - *Asset Management*
    - *Data Protection & Privacy*
    - *Access Control*
    - *Information System Acquisition, Development & Maintenance*
    - *Threat & Vulnerability Management*
    - *Business Continuity Management*

  Besides the goals of completing the gap analyses for the six (6) policies covered and subsequent implementation plans, the overarching outcome associated with this workstream is the gathering of real life challenges and implementation strategies used by pilot agencies during policy adoption. This document includes lessons learned and challenges overcome by the pilot agencies, which are broken down for each of the policies discussed.

- ***On-Site Visits*** – The on-site visit workstream was developed to provide direct assistance to twenty-one (21) agencies. Assistance was provided during two (2) meetings up to four (4) hours in length each. As selected by DIS, the agencies participating were spread out over the course of the policy guidance and training initiative. The first on-site visit typically acted as a level-setting meeting where D&T discussed policy adoption due dates set forth by DIS, strategies for implementing the policies, templates and how to work with them, and the ability provide guidance on an open questions or particular challenges that agencies are facing in conjunction with the State policies. The second on-site visit was question driven meeting where, based on the foundation established during the first meeting, agencies could ask questions related policy requirements on any of the thirteen (13) State policies. While direct guidance and training related to actual agency challenges was provided, the on-site visits were used as a vehicle to provide first-hand assistance to agencies during the process of identifying gaps, developing implementation plans and a review of the State policies. In addition to the pilot workshop workstream, specific lessons learned from the on-site visits were included as part of this document.

- ***Ongoing Assistance*** – DIS will continue to provide guidance in the form of video and textual materials made available on the DIS website (currently on the "Resources" page). The DIS website will be an important resource available for agencies to utilize for security updates, State activities and additional sources of information.

In addition to the templates published on the DIS website, the following materials can also be found published on the *Resources* tab:

- ***Policy Workshop Presentations*** – These PowerPoints were presented as part of the policy workshop workstream and are made available to agencies via the DIS website. For the ten (10) workshops, a unique presentation was posted for agencies to utilize which breaks down the main requirements of a particular policy, overall risks, challenges and potential solutions and a questions and response section that highlights answers from open ended questions directed towards the policies or DIS.
- ***Data Inventory Tool*** – The Data Inventory Tool is a Microsoft Excel spreadsheet developed to guide a business process owner (e.g., program area/data owners) through performing a data inventory analysis. The Data Inventory Tool provides agencies with a standardized method to document and classify the data collected and processed by various agency systems. For further details on The Data Inventory Tool and supplemental procedures, instructions and templates, please refer to the Resources tab of the DIS website under the Tools section.

In summation, the policy guidance and training initiative was comprised of the following activities:

Figure 1. Summary of workstreams

Work Stream	Number of Agencies Covered	Policies covered	Number of meetings	Total time with agencies	Level of Depth
Pilots	3	1. Asset Management 2. Data Protection & Privacy 3. Access Control 4. Information System Acquisition, Development & Maintenance 5. Threat & Vulnerability Management 6. Business Continuity Management	21	84	High
Policy Workshops	30	1. Asset Management 2. Data Protection & Privacy 3. Access Control 4. Information System Acquisition, Development & Maintenance 5. Threat & Vulnerability Management 6. Business Continuity Management 7. IT Risk Strategy 8. Mobile Security 9. HR & Security Awareness 10. Physical & Environmental Security	30	45	Medium
On-site Workshops	19	All thirteen (13) Statewide Information Security Policy	38	152	Low

2 Appendix B – Additional Guidance on Policy Implementation

2.1 Policy Adoption Preparation

For the adoption of the State information security policies, agencies have a variety of different options and methods towards implementation; however there is one common goal, *compliance*. There are three (3) strategies recommended based on DIS guidance. It is important to note that each strategy has its benefits and drawbacks and that a combination of strategies can be used based on the internal environment of the agency. In addition, the thirteen (13) State information security policies are considered minimum compliance requirements, and agencies can choose to be more secure in addition to a policy, but should be at least compliant with the current policies. As the policy champion, one should understand each of the strategies mentioned and adapt them in a manner that is better suited for the agency towards compliance.

1. ***Policy Mapping*** – The first strategy is geared for agencies that have maintained up-to-date policies and procedures which are implemented and followed by its agency employees. If that is the case, agencies can map the missing pieces or gaps from the new thirteen (13) State policies into their existing policies or procedures and continue to utilize the existing policies and procedures (with new additions). This strategy is geared to try and decrease the level of policy writing effort that is needed if current policies exist and are implemented successfully.
2. ***Adopt & Reference Policies and Align Procedures*** –In this situation, similar to the 'policy mapping' method, the agency can cover gaps from the new thirteen (13) State policies by amending their existing procedures and reference the State policies from the internal procedures. In addition, the strategy allows for the creation of new procedures that encompass the requirements from the State policies. An agency may continue to have existing policies in addition to referencing the State policies, but in this strategy, an agency is acknowledging that their existing and where applicable, new procedures, are in compliance with the State policies. The benefit for agencies is that instead of writing both policies and procedures, an agency will just align and reference their current and new procedures to the State policies to be in compliance.
3. ***Customization of State Policies*** – In this strategy, an agency should perform a detailed, line-by-line review of the thirteen (13) policies and customize the policy to fit the agency. Whether the agency combines policies to make one large policy or an information security program or leaves them separated as they exist currently. By going through each bullet of the policy, the agency is acknowledging what applies and does not apply based on their environment.

2.2 Information Security Policy Deployment Additional Guidance

After the completion of implementation plan(s), there are two (2) additional considerations for agencies:

- ***Risk Ranking of Gaps*** – If the agency has already not done so during the gap analysis, agencies should consider to risk-rank each of the identified gaps to create priorities towards implementation. The risk ranking of gaps will help an agency identify their biggest security vulnerabilities and help dictate the amount of effort needed, resources and budget that need to be allocated and the overall structure of the internal security program.
- ***Near Term Solutions to Track Long Term Implementations*** – Another consideration for agencies when risk ranking their gaps will be to ascertain whether remediation strategies are identified as short, medium or long-term solutions to overcome gaps. While the long-term solution may be the answer to completely remediate the gap, agencies should identify those nearer term solutions that lower the risk of exposure to incidents and create a security environment that has an acceptable level of risk.

The more an agency can do to lower the risk of threats, incidents and corruption of data until a permanent solution is in place, the greater chance an agency has to effective comply with the State policies.

Once approval is gained through executive management, the process of implementation of agency policies should commence, however, there are a few steps before the policy should be live in the agency environment.

1. Agencies need to determine what documentation gaps exist based on the gap analyses. Before implementation of a policy, the procedures associated with controls and requirements of the policies should be developed and distributed appropriately. Should an employee leave the agency, documented procedures allow the agency to continue with little interruption in their daily processes.
2. Supporting documentation to controls, such as access request forms, terminations forms, asset management forms, remote access forms, risk assessment templates, BIA templates, job failure forms, etc., should be created for effective implementation of new and existing processes.
3. Technical solutions, new applications and security enhancements should be implemented to address identified gaps. Building off the previous steps, these solutions should be accompanied with the proper documentation from a process and control perspective.
4. The final step of policy awareness and training ties the documentation requirement for controls together with an employee understanding of the changes made to policy and processes which helps for an effective policy adoption. When implementing policies, an agency can choose to do this last step simultaneously as the training is taking place (on the job training) or train employees for awareness and then implement the policy.

2.3 InfoSec Policies Awareness

In alignment with the DIS goals for policy implementation, the final step in in the process is policy awareness and training for agency personnel that coincides with new processes and solutions implemented. While the implementation of policies can be incremental between now and July 1, 2016, over the course of the workstream, the following are different strategies agencies were using or planned on using to provide policy awareness and training. The following provides awareness strategies with further explanations that can be applied for effective policy awareness and training for employees.

- ***Intranet Posting*** **–** At a minimum, new implemented policies should be posted internally to allow agency personnel the chance to review the policy at a given point. Having the policies posted in an area that is easily accessible internally can enhance the collective security knowledge of the agency.
- ***Security Slogan*** – An innovative approach revealed by several agencies was the introduction of a security slogan to help enforce the premise of consistently thinking about security during daily operations and normal business activities. For example, one agency was planning on using the slogan, *Security First*, which may likely be used in many security emails, posted visually and pushed from agency leadership to persuade personnel to consistently think about the security ramifications of their everyday actions. Once implemented, an example of the power a slogan can provide could be preventing an employee from clicking on a phishing email attachment or for an employee to think twice about sending confidential or restricted agency data via email without the proper encryption methods in place.
- ***Annual Employee Evaluation*** **–** Multiple agencies have mentioned that one effective method they have used in the past (and plan on using for the State policies) is to incorporate the certain requirements in the annual employee review process. At that time, personnel could be informed on a new policy or specific requirement section of the policy that was ready to implement and sign off to acknowledge their responsibilities related to security.
- ***Email*** – Agencies can use email announcements to target a specific section of the policy and/or audience to share a new requirement with to provide fast and targeted awareness. In addition, agencies could use email to send links to new policies, copy or send attachments of the policy itself or additional combinations that provides awareness agency personnel.
- ***Lunch & Learn Meetings*** – A commonly used method is to introduce a series of training meetings over lunch where it is a more relaxed atmosphere. The goal for this type of meeting is to introduce a condensed, targeted and easy to follow requirement which can be retained. Having the training over lunch (which can either be catered or individual brought in by employees, thus the brown bag title) provides a learning environment

that feels less mandatory and encourages collaboration among those in the room. A good exercise for this type of method is to introduce new processes.

- ***On-The-Job Training*** – One of the more effective ways for employees to comprehend, adapt and learn new security requirements from the policies is by learning on the job during daily operations. Given that the particular procedures associated with job functions and daily business operations will be drafted or modified the on the job training can come not only from the supervisor or manager, but also from the procedures to provide additional guidance. The on the job training provides employees with an opportunity to work through tangible processes rather than reading or learning from other approaches mentioned.
- ***Online Training*** – Whether offered on State contract, through another contracted third-party or internally developed, the agency could develop or implement online training for an effective means to train employees on security requirements. In addition, an assessment procedure (e.g. quiz, survey or electronic signature) can easily be added to an online training course which can correlate compliance with the training requirement.
- ***Certifications*** – Agency leadership and training coordinators could encourage employees to obtain external certifications (e.g. Sans Security Training Certification, CISSP, etc.) to help analyze and protect security measures implemented through the State policies. External training certifications can help enforce the latest security training offered as well as provide a new and refreshed take towards security related to different job areas and functions.
- ***Compliance Associated With Training*** – As mentioned in previous bullets, having an assessment procedure associated with training can further enforce security requirements and provide the agency training coordinator and security liaisons with a form of verification signaling that employees passed the training course. In addition, it also allows insight into agency employees who are failing to grasp a particular training module who might require a more personal understanding of the security requirements.
- ***Security Seminar*** – Similar in nature to an 'All Hands Meeting', an internal security seminar could be implemented that could require employees to attend sessions of security awareness and training related to the implementation of the State information security policies. This method provides agency leadership the chance to lead by example and address employees at the same time further enforcing the agency wide culture change that is associated with the State security requirements.
- ***Newsletter*** – Another simple idea multiple agencies have begun to implement is to insert a particular policy requirement into a weekly, bi-weekly or monthly newsletter already issued by the agency. In an effort to drive further awareness towards information security, IT has inserted a brief security tip, policy requirement, synopsis of an issue and other valuable lessons learned to the already circulated newsletter. While the newsletter is

not meant as a security announcement (although an agency could implement a strictly security related newsletter), the distribution channel to employees is already considered and this method provides another subtle reminder to further enhance security awareness and training.

- ***Training & Materials Availability*** – As much as possible based on the type of training requirement, security training and awareness materials, presentations and training modules should be available to agency employees for quick reference. In the event the employee feels the need to double-check a security requirement related to their daily job functions, the more references and resources available in an easily accessible manner, the better the agency can position itself towards an increased security awareness culture. Furthermore, If training modules could be easily repeated (even if that individual passed the training initially), this could provide yet another resource for employees to remain up to date on particular security requirements and feel more comfortable that their actions are not opening up the agency to potential vulnerabilities.
- ***Tiered Approach*** – One recommended security awareness and training technique is to publish new security requirements in waves over the course of the next two years towards the compliance date of July 1, 2016. After determining specific gaps and the level of risk associated with the gap, agencies should tier their awareness and training in a manner that employees can better absorb and adapt to the new policies. By implementing everything at once, the outcome may seem overwhelming to employees with policy requirements that are not retained to memory. Consider implementing a tiered approach that allows for a more gradual learning curve at first and builds towards harder and potentially culture changing requirement implementation.
- ***Pictorial Procedures*** – Procedures do not ordinarily have to be written in paragraph form in order for the point to be demonstrated. Another strategy agencies could use, depending on the nature of the process, is taking pictures to depict the procedures and show a tangible example of how the process works in real life. For example, an agency could use this approach for the sanitization process of laptops. In this situation, the pictures could be accompanied by a brief explanation, but the result of understanding the procedures could be the same.

3 Appendix C – Sample Roles and Responsibility Chart

State of South Carolina Policy Guidance Initiative
Roles and Responsibilities Chart
[AGENCY NAME – SAMPLE]

Policy Champion	**John Smith, Security Liaison**				
State of South Carolina Information Security Policies	**Policy Sections**	**Policy Deployment Team**	**Implementation Role(s)** (e.g., HR Team, Software Developer, 'Bob Smith', etc.)	**Implementation Responsibilities** (e.g., document the implementation plan, identify and implement remediation strategies, etc.)	**Revision and Approval** (i.e., key stakeholders to review and sign off policies)
Access Control	Access Management	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Linda Carter* – Human Resources *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team *Barbara Johnson* – Documentation Lead *Linda Carter* – Gap Analysis Team, Procedures Team *James Walker* – Implementation Lead, Procedures Team	*John Smith* – Coordinate meetings and perform gap analysis. Collaborate with James Walker to develop the policy implementation plan. *Barbara Johnson* – Gather existing policies and procedures. Support John Smith and James Walker to document of the gap analysis and the policy implementation plan. *Linda Carter* – Collaborate with John Smith to perform the gap analysis. Develop procedures for transferring Human Resources (HR) information to Information Technology (IT) department during recruitment, promotion, relocation or termination (if identified as a gap). *James Walker* – Document the policy implementation plan. Identify challenges and risks. Develop procedures and around access controls according to the gap analysis. Implementation of remediation strategies around access control. Training of IT staff based on the new processes and procedures.	*John Smith* – Security Liaison *Elizabeth Hill* – HR Director *David Perez* – Chief of Staff *Marshal Teach* – Agency Director

	Network Access Management	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead, Implementation Team *James Walker* – Procedures Lead, Gap Analysis Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. – Identify challenges and risks. *James Walker* –Collaborate with John Smith to perform the gap analysis. Develop procedures and around access controls according to the gap analysis. Implementation of remediation strategies around access control. Training of IT staff based on the new processes and procedures.	*John Smith* – Security Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Identity Management	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Linda Carter* – Human Resources *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion *Barbara Johnson* – Documentation Lead, Implementation Team *Linda Carter* – Gap analysis Lead, Procedures Team *James Walker* – Implementation Team, Procedures Team	*John Smith* – Coordinate meetings and the development of gap analysis and policy implementation plans. *Barbara Johnson* – Gather existing policies and procedures. Develop the implementation and remediation strategies. Document the detailed Implementation plan based on the gap analysis. *Linda Carter* – Perform the gap analysis. Develop procedures for transferring Human Resources (HR) information to Information Technology (IT) department during recruitment, promotion, relocation or termination (if identified as a gap). *James Walker* – Identify challenges and risks. Collaborate with Barbara Johnson to develop the policy implementation plan. Develop procedures and around access controls according to the gap analysis. Implementation of remediation strategies around access control. Training of IT staff based on the new processes and procedures.	*John Smith* – Security Liaison *Elizabeth Hill* – HR Director *David Perez* – Chief of Staff *Marshal Teach* – Agency Director

	Authentication	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team *Barbara Johnson* – Documentation Lead *James Walker* – Implementation Lead, Gap Analysis Team	*John Smith* – Coordinate meetings and perform gap analysis. *Barbara Johnson* – Document the gap analysis and the policy implementation plan. Gather existing policies and procedures. *James Walker* – Develop the implementation and remediation strategies. Identify challenges and risks. Collaborate with John Smith to perform the gap analysis.	*John Smith* – Security Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Emergency Access	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *James Walker* – Gap Analysis Team, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the gap analysis and the policy implementation plan. Gather existing policies and procedures. *James Walker* – Identify challenges and risks. Collaborate with John Smith to perform the gap analysis.	*John Smith* – Security Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Password Policy	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *James Walker* – Gap Analysis Team, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *James Walker* – Identify challenges and risks. Collaborate with John Smith to perform the gap analysis. Develop procedures and around access controls according to the gap analysis. Implementation of remediation strategies around access control.	*John Smith* – Security Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director

	Password Administration	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *James Walker* – IT, Network Services Manager	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *James Walker* – Gap Analysis Team, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *James Walker* – Identify challenges and risks. Collaborate with John Smith to perform the gap analysis. Develop procedures and around access controls according to the gap analysis. Implementation of remediation strategies around access control.	*John Smith* – Security Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
Asset Management	Asset Identification	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Daniel Green* – IT Director *Susan Thomas* – IT Asset Manager *Kevin Mitchell* – IT Procurement Manager	*John Smith* – Policy Champion, Gap Analysis Team *Barbara Johnson* – Documentation Lead *Daniel Green* – Gap analysis Team *Susan Thomas* – Gap analysis Team, Procedures Team, Implementation Team *Kevin Mitchell* – Gap analysis Team, Procedures Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Daniel Green* – Collaborate with John Smith to perform the gap analysis *Susan Thomas* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. Develop procedures and around asset management according to the gap analysis. Implementation of remediation strategies. *Kevin Mitchell* – Collaborate with John Smith to perform the gap analysis. Develop procedures in classifying or identifying newly procured IT assets. (if found as a gap)	*John Smith* – Security Liaison *Daniel Green* – IT Director *Marshal Teach* – Agency Director
Business Continuity Management	Contingency Planning	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Marshal Teach* – Agency Director *Kevin Wright* – Operations Manager	*John Smith* – Policy Champion, Gap Analysis Team *Barbara Johnson* – Documentation Lead, Implementation Team *Marshal Teach* – Gap analysis Team *Kevin Wright* – Gap	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Marshal Teach* – Collaborate with John Smith to perform the gap analysis. *Kevin Wright* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. Develop	*John Smith* – Security Liaison *Daniel Green* – IT Director *Kevin Wright* – Operations Manager *David Perez* – Chief of Staff *Marshal Teach* –

		Daniel Green – IT Director *Elizabeth Hill* – HR Director	analysis Team , Procedures Team, implementation *Daniel Green* – Gap analysis Team *Elizabeth Hill* – Gap analysis Team	procedures with respect to contingency planning according to the gaps identified. Implementation of the remediation strategies for contingency planning. *Daniel Green* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Elizabeth Hill* – Collaborate with John Smith to perform the gap analysis.	Agency Director
	Disaster Recovery and Contingency Strategies	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Kevin Wright* – Operations Manager *Daniel Green* – IT Director *Carol Anderson* – *Communications Manager*	*John Smith* – Policy Champion / Gap Analysis *Barbara Johnson* – Documentation Lead *Kevin Wright* – Gap analysis Team, Implementation Team *Daniel Green* – Gap analysis Team, Implementation Team *Carol Anderson* – Gap analysis Team, Procedures Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Kevin Wright* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Daniel Green* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Carol Anderson* – Collaborate with John Smith to perform the gap analysis. Develop and implement procedures for communication during disaster recovery (if found as a gap).	*John Smith* – Security Liaison *Daniel Green* – IT Director *Kevin Wright* – Operations Manager *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Data Backups	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Kevin Wright* – Operations Manager *Daniel Green* – IT Director	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *Kevin Wright* – Gap analysis Team , Implementation Team *Daniel Green* – Gap analysis, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Kevin Wright* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Daniel Green* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks.	*John Smith* – Security Liaison *Daniel Green* – IT Director *Kevin Wright* – Operations Manager *David Perez* – Chief of Staff *Marshal Teach* – Agency Director

Data Privacy & Protection	Data Classification	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Jennifer Adams* – Privacy Liaison *Sharon Anderson* – Data Analyst *Daniel Green* – IT Director	*John Smith* – Policy Champion, Gap Analysis Lead *Barbara Johnson* – Documentation Lead / Implementation Lea *Jennifer Adams* – Gap analysis Team *Sharon Anderson* – Data champion *Daniel Green* – Gap analysis Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Jennifer Adams* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Sharon Anderson* – Perform data classification according to the schema. Complete the data inventory tool. *Daniel Green* – Collaborate with John Smith to perform the gap analysis. .	*John Smith* – Security Liaison *Daniel Green* – IT Director *Jennifer Adams* – Privacy Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Data Disposal	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Jennifer Adams* – Privacy Liaison *Daniel Green* – IT Director	*John Smith* – Policy Champion, Gap Analysis Lead, Implementation Lead *Barbara Johnson* – Documentation Lead *Jennifer Adams* – Gap analysis Team, Implementation Team *Daniel Green* – Gap analysis, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Jennifer Adams* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Daniel Green* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks.	*John Smith* – Security Liaison *Daniel Green* – IT Director *Jennifer Adams* – Privacy Liaison *David Perez* – Chief of Staff *Marshal Teach* – Agency Director
	Data Protection	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Jennifer Adams* – Privacy Liaison *Daniel Green* – IT Director	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *Jennifer Adams* – Gap analysis Team, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Jennifer Adams* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. *Daniel Green* – Collaborate with John Smith to perform	*John Smith* – Security Liaison *Daniel Green* – IT Director *Jennifer Adams* – Privacy Liaison *David Perez* – Chief of Staff

			Daniel Green – Gap analysis Team, Implementation Team	the gap analysis. Identify challenges and risks.	*Marshal Teach* – Agency Director
	Privacy	*John Smith* – Security Liaison *Barbara Johnson* – Technical Writer *Jennifer Adams* – Privacy Liaison *Daniel Green* – IT Director	*John Smith* – Policy Champion, Gap Analysis Team, Implementation Team *Barbara Johnson* – Documentation Lead *Jennifer Adams* – Gap analysis Team, Implementation Team, Procedures Lead *Daniel Green* – Gap analysis Team, Implementation Team	*John Smith* – Coordinate meetings and perform gap analysis. Develop the implementation and remediation strategies. *Barbara Johnson* – Document the detailed Implementation plan based on the gap analysis. *Jennifer Adams* – Collaborate with John Smith to perform the gap analysis. Identify challenges and risks. Develop procedures to perform Privacy Impact Analysis (PIA) (if found as a gap) and perform a PIA. *Daniel Green* – Collaborate with John Smith to perform the gap analysis.	*John Smith* – Security Liaison *Jennifer Adams* – Privacy Liaison *Marshal Teach* – Agency Director

***NOTE**: The above Roles & Responsibilities Chart example only covers the first four (4) policies in the template, whereas agencies are required to complete all policy sections in the template.*

Challenges Defining Roles and Responsibilities

Limited Staff – Some agencies operate with limited staff and in small environments. It is understood and acceptable to identify the same individual as responsible for multiple sections and multiple roles for policy adoption. When completing the roles and responsibilities chart, be sure to thoroughly analyze the policy topics and determine whether or not there are personnel with higher level of knowledge that can participate on this effort.

Lack of Agency Leadership Commitment – In order for agencies to effectively adopt the State's information security policies, it is imperative to have support from executive leadership. Without support from the top, policies cannot be adopted and operationalized effectively. Through collaboration between DIS and the Agency, executive management should have a clear understanding of the policy compliance initiative and fully support the policy deployment teams in their effort to identify gaps and implementation strategies. This handbook can be used as a tool to help leadership understand the vast nature this process and the detailed steps it takes to analyze the current environment and plan for remediation. *Refer to Step 2, InfoSec Executive Management Approval & Policies Implementation for further details.*

4 Appendix D – Sample Gap Analysis – Asset Management

Gap Analysis to Support the Implementation of the South Carolina

Asset Management Policy

The below Gap Analysis is developed based on the feedback provided by the policy implementation team of the (SC SAMPLE State Agency). The table outlines the policy requirements (procedures, standards and policies which may/may not be implemented), relevant questions to address and identify gaps in the agency's environment.

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
InfoSec Policy has been reviewed and approved by the key stakeholders.	**Has the InfoSec Policy been reviewed and approved by the key stakeholders?**	**No**	**AM 1: The Asset Management policy has not been reviewed and approved by key stakeholders.**	**To be completed once the "Asset Management Policy" is adopted or documented.** **Brainstorming: Key stakeholders would include: John Smith – ISO** **Daniel Green – IT Director** **Marshal Teach - Agency Director**
InfoSec Policy has been approved and received sign off by the authorized executives.	**Has the policy been approved and received sign off by the authorized executive?**	**No**	**AM 2: The Asset Management policy has not been approved and signed off by authorized executives**	**To be completed once the "Asset Management Policy" is adopted or documented, reviewed and approved.** **Brainstorming: Have internal meetings before sharing with Agency director. Key stakeholders should sign off before moving forward to Director.**
The policy has been socialized across the Agency for personnel	**Has the policy been shared with all personnel across-**	**No**	**AM 3: The Asset Management policy has not been socialized across the agency.**	**To be completed once the "Asset Management Policy" is documented, reviewed, approved and signed off.**

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
awareness.	**Agency?**			**Need to determine training style for each process and procedure of the policy, as well as an overall method for the policy itself.** **Brainstorming: All documentation will need to be in place before we can push out training.** **Open Question: Should we post to the intranet? SharePoint? File Share Drive? Other?**
Documented Asset Management Policy.	Does your Agency have a documented Asset Management Policy?	No	AM 4: Asset Management Policy not documented	The agency follows certain procedures for asset management but nothing is documented so far.
	Is the policy aligned with the State of South Carolina Asset Management Policy?	Partial	AM 5: The Asset Management Policy is not aligned with the Statewide Policy	Gap analysis and implementation plans will be conducted to align the same.
Implemented Asset Management Policy and associated processes	Have you implemented an Asset Management Policy?	No	AM 6: Agency lacks a formalized Asset Management policy.	Need to align the existing procedures with the policy
	Do you have asset management processes implemented in your Agency? (i.e. asset inventory creation and review, asset registration, asset classification, user provisioning, etc.)	Partial	• AM 7: Processes and documented procedures are not developed to track software, service and information assets. In addition, physical asset processes and procedures should be further aligned to the asset management policy. • AM 8: Assets are not classified into various categories.	The agencies track physical assets through the agency asset inventory (An Access Database). The agency is looking to procure a solution that can be used to replace the existing asset inventory. SCIES also used to track assets valued over $1500. Processes exists asset registration, user provisioning etc.

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
			• AM 9: The agency does not have established processes and documented procedures for the following: 1. New asset requests/Asset registration 2. Asset classification 3. User provisioning associated with assets 4. Asset inventory review 5. SCEIS inventory reconciliation process 6. Others TBD – as needed	
Document and maintain asset inventory for critical IT assets.	Have you identified asset owners?	Partial	AM 10: Asset owners are not identified for each type of asset: physical, software, service and information assets.	Asset owners identified for physical assets (e.g. such as asset owners for computers). There is a need to document the asset owners for the other 3 types of assets. Open Question: Do we want to have asset owners that oversee the categories of assets (e.g. an individual responsible for monitoring physical assets)?
	Does your Agency have an asset inventory?	Partial	AM 11: A centralized asset inventory is not established to manage the 4 types of assets (e.g. physical, software, service and information assets).	Asset inventory has been created for physical assets.
	Have critical assets been identified within your asset inventory?	Partial	AM 12: Critical assets need to be documented and centrally documented within the developed	Agency has identified information assets containing sensitive information. The Asset inventory classifies the type of information handled by the asset.

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
			procedures.	Critical assets are known by IT; however, they are not documented and written down. Open Question: Is there a need to conduct a BIA to validate the critical access component?
Asset inventory that is inclusive of the unique system name, a system/business owner, a data classification, and a description of the location of the asset.	Do you have an asset management team?	Yes	No Gap – Compliant	The agency has an Asset Inventory Manager who keeps track of the physical assets. Need to make sure that other assets are also tracked during this process.
	Who assigns asset management team's roles and responsibilities?	Yes	No Gap – Compliant	Susan Thomas – IT Asset Manager Susan mentioned that she is aware of her responsibility, but will need to be trained on new processes and procedures associated with the other type of assets.
	If you have an asset management team, what are the team's roles and responsibilities?	Partial	AM 13: Roles and responsibilities of asset owners are not formally documented	There is nothing formally documented. The IT asset manager understands the roles and responsibilities. The team tracks existing IT assets, all the way from procurement to disposal. The also keep track of the chain of custody of these IT assets. Training needs to be accompanied with new responsibilities.
	If you have an asset inventory, does it include a unique system name, a system/business owner,	Partial	• AM 14: The asset inventory does not include software, service and information assets identified with unique names, system/business owner, data classification and	The asset inventory currently includes a system tag, asset owner, type of data contained but only done for physical assets. However it does not classify the type of asset and does not specify the location of the assets.

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
	a data classification, and a description of the location of the asset? *Examples of assets associated with information systems are (information/software/physical assets and services).*		location. • AM 15: The physical assets (currently documented) do not include the location and type of asset in the asset inventory.	
Access to assets granted via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.	Are there controls in place to restrict access to asset inventory to approved individuals only? (e.g., user credentials, user roles, etc.)	Yes	No Gap – Complaint	Currently only the IT Asset Manager, the DBA and the Network Sys Admin have access
	Is access to asset inventory a documented process?	No	AM 16: There is no documented process in place to provide access to the asset inventory.	Only the three individuals above have access to the asset inventory. For reporting purposes the IT asset manager creates a report for socializing with departments and higher management Open Question: Is this going to be part of the new hire request form being created? Should we keep this separate?
	Do you require users to acknowledge rules and regulations pertinent to the asset?	Yes	No Gap – Complaint	For the IT, assets the Users are required to acknowledge the pre login message for the agency owned assets. The message highlights that “By accessing and using this system you are consenting to the agency’s acceptable use policy.” The acceptable use policy highlights the rules and

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
				regulations of using agency IT assets. Open Question: Do we need a separate form for asset acknowledgment or rules and regulations? Is the acceptable use policy up to date?
Periodically revalidate asset inventory to ensure accurate classification.	Is there a periodic review of the asset inventory performed to help ensure accuracy?	No	AM 17: There is not a defined process for the periodic review of the asset inventory to help ensure accuracy.	No review process in place yet. Brainstorming: Need to document complete asset inventory first and gather input from Susan related to how this process will work.
	Has responsibility for the periodic reviews been assigned to a specific role/ individual?	No	AM 18: The role of periodically reviewing assets has not been assigned, documented or trained.	Responsibility to be assigned to the IT Asset Manager or Internal Audit Team Brainstorming: Need to document all processes and procedures prior to a review taking place. This one is especially dependent on others.
	Is the asset inventory review process documented?	No	AM 19: A documented process to internally review the asset inventory does not exist.	Currently the changes made to the asset inventory are logged. May be these changes could be utilized in the review process.
Establish procedures to administer privileged user accounts in accordance with a role-based access model.	Have you established procedures to administer privileged user accounts based on employees' roles?	Partially	AM 20: Procedures have not been established to administer privileged user accounts to employees based on asset management roles.	Currently only the IT Asset Manager, the DBA and the Network Sys Admin have access. All of them have administrative roles. The activities are monitored through logging of changes.
Classify assets into the data classification types in the State of South Carolina Data	Are you familiar with the State of South Carolina Data Classification Schema?	Yes	No Gap – Compliant	

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
Classification Schema.	Has a data classification schema been implemented at your agency?	No	AM 21: The data classification schema is not implemented within the agency.	The data classification schema is not implemented, however the IT assets are classified based on the type of information contained. Brainstorming: Need to gather assets before classification exercise. Open Question: Can we leverage the data inventory tool posted on DIS website to help with classification Open Question: Do we want to use these bullets in the data protection & privacy implementation plan?
Assets are classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.	How do you classify asset data in the asset inventory?	Gap identified	AM 22: The asset inventory needs to be aligned to the State of South Carolina data classification schema.	Based on the type of information contained in the asset
	Is the asset data classified based on type and impact levels in the asset inventory?	Gap identified	See above	The data classified was used to identify critical, sensitive, essential and normal assets within the agency Open Question: Are all assets identified with type and impact level? Do we need to consider this an actual gap or process improvement?

Challenges Conducting Gap Analyses

Interpretation of Policy Requirements – While reviewing the gap analyses and familiarizing yourself with the policy sections, there are bound to be requirements that are open to interpretation, further analysis or require follow-up questions to help clarify the policies. When a question from the gap analysis arises, the first thing a policy champion should do is to refer back to the State policy. When in doubt, the State policy will be the baseline requirement and thus, one should defer to how the policy requirement (or bullet) reads. If further clarification is required, the DIS inbox is an excellent resource to leverage, informationsecurity@bcb.sc.gov. Between reviewing the policy and reaching out to DIS to clarify the requirement and an agency's circumstances, the agency will be able to get the proper answer to help interpret the policies.

Documentation Gaps vs Process Gaps – There are two different types of gaps that agencies should identify when completing the gap analyses. Process gaps are a more common type and identify those processes that are not in compliance to the State policies. For instance, the Access Control policy states that agencies shall implement 'periodic user access reviews'. If access reviews do not take place at your agency, then you have a process gap.

Documentation gaps are the often forgotten step of the analysis, but are equally important. Documentation gaps consist of whether the particular requirement or process has the proper underlying procedures and subsequent forms, templates, etc. If the answer to this question is *no*, then agencies should document a separate gap for documentation. To continue the example used earlier, if the agency does not have a user access review process, they have a process *and* documentation gap. Thus the agency may likely have to document the procedures they are going to use and forms, templates or supporting documentation to help with the process. If the agency has a user access review process that is currently in place, but does not have the procedures documented, they may likely write a documentation gap only on the gap analysis and transfer that to the implementation plan.

This analysis for agencies to align themselves to the State policies is going to be a documentation exercise, thus, there should be multiple documentation gaps on each finalized gap analysis template. A requirement is only considered ready for implementation when the underlying and supporting documentation is completed.

Do Not Get Caught in the Details of Requirements – The State policies were drafted and designed to be adoptable by all agencies in the State. Because of that notion, there is lots of room for agencies to determine what compliance means based on their environment against particular requirements. The goal is to not get caught analyzing specific details and repercussions of the requirements, but rather understanding how it fits into the agencies environment. For example, in the IT Risk Management policy, there are two requirements that mention agencies shall have a Corrective Action Plan (CAP) and a Plan of Actions & Milestones (POAM) document. A CAP can be considered an assessment focused on one system or one area, while a POAM is more to shape the culture of the agency. A POAM might consist of multiple CAPs. Upon research, templates for these documents are very similar and one could argue that they could be combined rather than keeping them separate, which is exactly the point of this challenge. If an agency can justify that they have the pieces of the CAP combined into a larger POAM and only use the POAM in their environment, that is an acceptable response. Agencies should not be caught scrutinizing specific details, but rather take each of the requirements and understand the nature to which the requirement is trying to help enhance security to determine whether gaps exist in their environment.

5 Appendix E – Sample Implementation Plan – Asset Management

Policy Implementation Plan of Action

[Asset Management Policy]

The below Policy Implementation Plan of Action is developed based on the feedback provided by the policy implementation team of the (SC State Agency). The table references the policy clauses, gaps identified through the gap analysis, implementation challenges and implementation strategy which the (SC State Agency) will develop and implement in their environment.

Legend

'IP' = 'In Progress'

'SAR' = 'Specific Action is Required'

'IM' = 'Implemented'

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
InfoSec Policy has been reviewed and approved by the key stakeholders.	**AM1: The Asset Management policy has not been reviewed and approved by key stakeholders.**	➢ **The Asset management Policy has not been documented**	**1. Once the Asset Management policy is drafted, submit the Asset Management policy for review and approval from key stakeholders (Daniel Green and Marshal Teach)**	**John Smith - ISO**	**IP**	***To be submitted for review by 10/31/2014*** ***To be Approved by 11/07/2014***
InfoSec Policy has been approved and received sign off by the authorized executives.	**AM2: The Asset Management policy has not been approved and signed off by authorized**	➢ **The Asset management Policy has not been documented** ➢ **The Asset**	**1. Once the Asset Management policy is reviewed and approved by the key stakeholders, submit the Asset Management policy for approval and sign off by the**	**John Smith - ISO**	**IP**	***To be submitted to executives by 11/7/2014*** ***To be signed off by 11/15/2014***

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
	executives	**Management Policy Draft has to go through the review and approval process**	**authorized executives(Marshal Teach)**			
The policy has been socialized across the agency for personnel awareness.	**AM3: The Asset Management policy has not been socialized across the agency.**	➢ **The Asset management Policy has not been documented** ➢ **The Asset Management Policy Draft has to go through the review and approval process** ➢ **The Asset Management policy has not been approved and signed off.**	**1. Once the Asset Management policy is reviewed and signed off by the authorized executives, upload the policy to the agency SharePoint website.** **2. Conduct an agency wide training and awareness session on Asset Management**	**John Smith - IO**	**IP**	**1. To be uploaded to SharePoint by 11/15/2014** **2. Start Conducting the agency wide training and awareness sessions 11/30/2014** ***The gap to be closed by 12/31/2014***
Documented Asset Management Policy.	AM 4:Asset Management Policy not documented	N/A	1. Begin drafting the Asset Management Policy with reference to the Statewide Asset Management policy published by DIS *(refer to AM1 & AM2)*	Barbara Johnson - Technical Writer	IP	1. 9/21/2014
Documented Asset Management Policy.	AM 5: The Asset Management Policy is not aligned with the Statewide Policy	➢ Procedures needs to be realigned with the Statewide Asset Management Policy requirements	**1. Conducted the Gap Analysis** **2. Developed the remediation plan, based on the gap analysis**	Susan Thomas – IT Asset Manager	IP	**1. Gap Analysis finalized on 5/31/2014**

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
		➢ Need to redefine certain processes based on the requirements in the agency	3. Perform remediation activities based on the implementation plan			**2. Implementation Plan finalized on 6/31/2014** 3. To be completed by 12/31/2014 *Gap to be closed by 12/31/2015*
Implemented Asset Management Policy and associated processes	AM 6: Agency lacks a formalized Asset Management policy.	➢ Procedures needs to be realigned with the Statewide Asset Management Policy requirements ➢ Need to redefine certain processes based on the requirements in the agency	1. Document realigned and redefined processes and procedures. 2. Implement these realigned and redefined procedures by institutionalizing the policy and socializing with appropriate agency staff	Susan Thomas – IT Asset Manager	IP	1. Document Redefined/realigned process and procedures by 06/31/2015 2. Implement processes and procedures and socialize by 12/31/2015 *Gap to be closed by 12/31/2015*
Implemented Asset Management Policy and associated	AM 7: Processes and documented procedures are not	➢ Current Asset inventory needs to be overhauled to include	1. SHORT TERM: Edit the current asset inventory and enable it to track software, service and	Susan Thomas – IT	IP	1. Edit existing inventory by 2/28/2015

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
processes	developed to track software, service and information assets. In addition, physical asset processes and procedures should be further aligned to the asset management policy.	software, service and information assets. ➢ Agency may need migrate to a new asset management solution in the long run	information assets 2. SHORT TERM: Identify sources of data for software, service and information assets by conducting meetings with the required teams, IT Services, Procurement Services etc. 3. SHORT TERM: Conduct an inventory count for the existing software, service and information assets from the identified sources 4. SHORT TERM: Define and implement processes and procedures to track software, service and information assets similar to physical assets 5. LONG TERM: Conduct Vendor assessment to find a suitable asset management solution and request and RFP for the same.	Asset Manager		2. Sources to be identified by 3/15/2015 3. Inventory count to be updated by 4/30/2015 4. Define processes and procedures by 6/31/2015 5. Conduct vendor assessment by 10/31/2015 and submit RFP by 12/31/2015 *Gap to be closed by 12/31/2015*
Implemented Asset Management Policy and associated processes	AM 8: Assets are not classified into various categories.	N/A	1. SHORT TERM: Edit the current asset inventory and enable it to categorize assets into various categories 2. LONG TERM: Conduct Vendor assessment to find a suitable asset management solution and request and RFP for the same.	Susan Thomas – IT Asset Manager	IP	1. Edit existing inventory by 2/28/2015 2. Conduct vendor assessment by 10/31/2015

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
						and submit RFP by 12/31/2015 *Gap to be closed by 12/31/2015*
Implemented Asset Management Policy and associated processes	AM 9: The agency does not have established processes and documented procedures for the following: 1. New asset requests/Asset registration 2. Asset classification 3. User provisioning associated with assets 4. Asset inventory review 5. SCEIS inventory reconciliation process *Others TBD – as needed*	N/A	Develop and Establish processes and documented procedure for: 1. Asset classification 2. SCEIS inventory reconciliation process 3. New asset requests/Asset registration 4. User provisioning associated with assets 5. Asset inventory review	Susan Thomas – IT Asset Manager	IP	1. 2/28/2015 2. 4/30/2015 3. 6/31/2015 4. 6/31/2015 5. 6/31/2015 *Gap to be closed by 6/31/2015*
Document and maintain asset	AM 10: Asset owners are not identified for	➢ Assets need to be classified and asset	1. Identify asset owners for each item in the asset inventory (after	Susan Thomas	IP	*Gap to be closed by 10/31/2015*

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
inventory for critical IT assets.	each type of asset: physical, software, service and information assets.	inventory needs to be updated for identifying asset owners ➢ Training and awareness for asset owners on how to handle assets	incorporating software, service and information assets into it) 2. (individual owners for physical assets, single owners for software, service and information assets)	– IT Asset Manager		
Document and maintain asset inventory for critical IT assets.	AM 11: A centralized asset inventory is not established to manage the 4 types of assets (e.g. physical, software, service and information assets).	➢ Assets need to be classified and asset inventory needs to be updated	1. Edit and update the current asset inventory and enable it to track software, service and information assets	Susan Thomas – IT Asset Manager	IP	*Gap to be closed by 4/30/2015*
Document and maintain asset inventory for critical IT assets.	AM 12: Critical assets need to be documented and centralized within new procedures.	➢ Assets need to be classified and asset inventory needs to be updated	1. Schedule a meeting with stakeholders to document the critical assets (Note: IT Services, Network and System Managers have already identified the critical assets based on the sensitivity of the data present on the asset) 2. Update the asset inventory with the critical IT assets identified and documented as part of the discussion. (this can be done by adding an extra field in the asset inventory to tag critical assets)	Susan Thomas – IT Asset Manager	IP	1. Meeting to be completed by 3/31/2015 2. Inventory to be updated with critical assets by 4/30/2015 *Gap to be closed by 4/30/2015*
Asset inventory that is inclusive of the unique system	AM 13: Roles and responsibilities of asset owners are not	➢ Need to identify asset owners for software, service and	1. Document roles and responsibilities of asset owners	Susan Thomas – IT	IP	*Gap to be closed by 6/31/2015*

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
name, a system/business owner, a data classification, and a description of the location of the asset.	formally documented	information assets		Asset Manager		
Asset inventory that is inclusive of the unique system name, a system/business owner, a data classification, and a description of the location of the asset.	AM 14: The asset inventory does not include software, service and information assets identified with unique names, system/business owner, data classification and location.	➢ Assets need to be classified and asset inventory needs to be updated	1. SHORT TERM: Edit and update the current asset inventory and enable it to track software, service and information assets 2. LONG TERM: Conduct Vendor assessment to find a suitable asset management solution and request and RFP for the same *(refer to AM8)*	Susan Thomas – IT Asset Manager	IP	*Gap to be closed by 4/30/2015*
Asset inventory that is inclusive of the unique system name, a system/business owner, a data classification, and a description of the location of the asset.	AM 15: The physical assets (currently documented) do not include the location and type of asset in the asset inventory.	N/A	1. Edit the current asset inventory and enable it to track type and location of the asset 2. Update the current asset inventory with the type and location of the asset	Susan Thomas – IT Asset Manager	IP	1. Edit existing inventory by 2/28/2015 2. Inventory count to be updated by 4/30/2015 *Gap to be closed by 4/30/2015*
Access to assets granted via a formal registration process that requires user	AM 16: There is no documented process in place to provide access to the asset	N/A	1. Define user roles for the access. 2. Develop and implement process to provision access for new users to access the asset inventory	Susan Thomas – IT Asset	IP	1. Define user roles by 3/30/2015

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
acknowledgement of all rules and regulations pertinent to the asset.	inventory. (Only the three individuals have access to the asset inventory.)		3. Document the process and the roles and responsibilities of various user roles 4. Develop a training curriculum for users (role specific) describing roles and responsibilities	Manager		2. Define processes and procedures by 6/31/2015 3. Document processes and roles and responsibilities by 6/31/2015 4. Develop a training curriculum by 8/31/2015 *Gap to be closed by 8/31/2015*
Periodically revalidate asset inventory to ensure accurate classification.	AM 17: There is not a defined process for the periodic review of the asset inventory to help ensure accuracy.	➢ Asset inventory needs to be updated with all types of assets including physical, software, service and information assets	1. Develop and implement procedures for periodic review of asset inventory 2. Document the procedure for periodic review of asset inventory	Susan Thomas – IT Asset Manager	IP	1. Define processes and procedures by 6/31/2015 2. Document processes and procedures by 6/31/2015 *Gap to be closed by 6/31/2015*

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
Periodically revalidate asset inventory to ensure accurate classification.	AM 18: The role of periodically reviewing assets has not been assigned, documented or trained.	➢ Asset inventory needs to be updated with all types of assets including physical, software, service and information assets before the periodic review.	1. Designate the role of periodic review of assets – Role designated to Internal Audit Team (Joseph Mathews –IA Lead) 2. Define and document roles and responsibilities (including frequency) for personnel doing periodic review 3. Conduct training session for the personnel doing periodic review	Joseph Mathews – Internal Audit Lead	IP	1. Designated the role on 6/31/2014 2. Document processes and roles and responsibilities by 6/31/2015 3. Train the personnel by 9/30/2015 *Gap to be closed by 9/30/2015*
Periodically revalidate asset inventory to ensure accurate classification.	AM 19: A documented process to internally review the asset inventory does not exist.	➢ Asset inventory needs to be updated with all types of assets including physical, software, service and information assets	1. Develop and implement procedures for periodic review of asset inventory 2. Document the procedure for periodic review of asset inventory	Susan Thomas – IT Asset Manager	IP	1. Define processes and procedures by 6/31/2015 2. Document processes and procedures by 6/31/2015 *Gap to be closed by 6/31/2015*
Establish procedures to administer	AM 20: Procedures have not been established to	➢ Currently there are only administrator roles.	1. Develop and implement process and procedure to administer privileged accounts related to	James Walker – IT,	IP	1. Define processes and

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
privileged user accounts in accordance with a role-based access model.	administer privileged user accounts to employees based on asset management roles.	➢ Other user access roles have to be defined	asset inventory. 2. Document the procedure to administer privileged accounts. 3. LONG TERM: Agency may need to look at a Privileged User Management (PUM) Solution.	Network Services Manager		procedures by 6/31/2015 2. Document processes and procedures by 6/31/2015 3. Request RFP for PUM by 12/31/2105 *Gap to be closed by 12/31/2015*
Classify assets into the data classification types in the State of South Carolina Data Classification Schema.	AM 21: The data classification schema is not implemented within the agency.	➢ Need to implement the State Data Classification Schema	1. Utilize the State Data inventory tool and data classification tool and perform data classification based on that. *Note: Refer to Gaps DP 12, 13 and 16 for implementation plan associated with data classification and implementation of the data inventory tool.* 2. Use the state data classification guidelines in updating the asset inventory.	Sharon Anderson – Data Analyst	IP	1. Data classification to be performed by 3/31/2015 2. Update the asset inventory by 4/30/2015 *Gap to be closed by 4/30/2015*
Assets are classified based on data classification type and impact level, and the appropriate level of information security safeguards	AM 22: The asset inventory needs to be aligned to the State of South Carolina data classification schema.	➢ Need to implement the State Data Classification Schema	1. Use the state data classification guidelines in updating the asset inventory. 2. Use the data inventory tool to classify asset data	Susan Thomas – IT Asset Manager	IP	1. Update the asset inventory by 4/30/2015 2. Update the asset

Implementation Plan						
Related Policy Clause	**Current Gaps**	**Implementation Challenges**	**Implementation Strategy**	**Lead**	**Status**	**Due Date**
are available and in place.						inventory by 4/30/2015 *Gap to be closed by 4/30/2015*

Challenges Developing Implementation Plans

Format that Works for You – Implementation plans are meant to be living documents that are continually maintained, updated and tracked until all gaps are remediated. One of the biggest factors in managing implementation plans is coming up with a format (e.g. the columns, numbering scheme, color coding, merging of cells, application format and other formatting changes) that is comfortable for parties to read, understand and react promptly. While the template posted on the DIS website and outlined in Appendix D is presented in Word, where an agency documents implementation plans is their decision for what works well for the agency. Important columns of the implementation plan are 'Gaps' and 'Strategy' as they form the basis of the exercise. Given that policy deployment teams will be leveraging the implementation plans until at least 7/1/2016 and potentially beyond, agreeing on the effective columns, how effectively to track gap remediation leaders, how to document updates and similar thoughts play a huge role in effectively staying on top of the current status. Perhaps agencies find that very detailed, granular level implementation plans work better for day to day maintenance, whereas a high-level summary implementation plans or reports work better for executive management updates. In the end, get comfortable with the formatting of the implementation plan so that when someone revisits a particular policy, section or gap, there will be no time lost trying to remember what the gap is or the current status.

Not Knowing What Strategy – A common challenge when developing implementation plans is that an agency might now know what the strategy is for how they plan to remediate a particular gap. Agencies are simply encouraged put down what the strategy is at a given point in time. As implementation plans are rarely considered final (until all gaps are remediated), the strategy associated with gaps will change based on current or future knowledge of the agency. If the strategy is 'need to research vendors' with a due date in October 2014, once the research has concluded, the agency should upload the new steps to remediate the gap based on what they found out through researching vendors. Perhaps the agency selected an agency and now has to 'schedule meeting with vendor x to….', 'coordinate internally to design procedures', ' document new processes', and 'train employees on implementation of xyz application'. The

point is that an agency will not have a clear picture of how they plan to overcome each gap on the first draft of an implementation plan. The goal will be to continually update and monitor to implementation to add strategies and stay on track with self-imposed due dates. *See Challenge #4 – Due Dates below for further details on managing implementation plans.*

The Amount of Details That Need to be Included – Again, this challenge is completely dependent on the amount of detail an agency feels is required to understand the gap, strategy to overcome that gap and additional columns which provide further clarifications. At a minimum, the gap itself should be detailed enough that you can understand it out of context of looking at other gaps or the gap analysis question. A gap should be clear, detailed and easy to understand exactly what is missing in the current environment. The strategy to remediate the gap should also be detailed with different steps and individual due dates. The more details an agency can include the better chance of tracking and meeting due dates and overall goals the agency has with managing implementation plans. The goal should be for an agency to include the level of detail that makes the implementation plan manageable not only by the policy deployment teams, but also executive management awareness.

Not Knowing Due Dates Associated with Remediation Strategies – This challenge is perhaps the toughest, but again, is very manageable as long as the agency has found an implementation plan that is designed, formatted and managed in a routine manner. The reason for assigning individual due dates for each strategy step to close a single gap (rather than one end goal date) is to create daily, weekly or monthly checkpoints for the agency to manage. It is much easier to manage tasks (remediation strategy steps) on defined intervals to stay on track from a project management perspective. It is important to note that dates should rarely feel final and can be adjusted week to week or month to month based on current circumstances. Individual dates are only meant to help internally manage the workload for policy deployment teams. The suggestion may likely be to put dates that you think are realistic and then adjust as the environment changes, further details are learned or other circumstances arise. For instance, a long-term strategy such as 'implementation of asset management solution' which requires research, budget and planning could have an individual date of 2/1/2016 (a date well into the future). When that date arrives, the policy deployment team might move the date further, adjust slightly or completely remove the strategy but the point is at that date, they will have a better idea of where the agency stands and can make the proper adjustments. Individual due dates can also help you sort by resource to see if a particular week or month is overloaded for that employee and can adjust accordingly. Due dates rarely have to be considered final and can be continually adjusted, but they will help the agency maintain an on track schedule to remediate gaps until the final compliance date, July 1, 2016.

6 Appendix F – Lessons Learned: Information Security Policy Deployment

6.1 InfoSec Policies Development Strategies

DIS, provided additional support to selected agencies through the following activities and associated materials:

- Policy Workshops – Policy workshops were conducted twice per month covering ten (10) State policies with thirty (30) agency policy champions.
- Pilot Workshops – Guiding three (3) agencies through six (6) policies by conducting joint gap analyses, helping to fill out and review completed documentation and start building the foundation for implementation plans against the gaps identified.
- On-Site Visits – Direct assistance to twenty-one (21) agencies selected by DIS for two (2) meetings up to four (4) hours in length.

Policy workshops formed the basis of the analysis in this section and thus, the first ten (10) policies are documented with considerations. For questions associated with the Master, IT Risk Management and IT Compliance policies or the below policies, please reach out to the DIS email, infomrationsecurity@bcb.sc.gov, for further guidance.

The following sections break down the approach used during the Pilot workshops that the Large, Medium and Small Agencies utilized towards the completion of the various templates (Roles and Responsibilities Chart, Gap Analysis and Implementation Plans) and the strategy for policy adoption and implementation. Large, Medium and Small agencies were broken out by DIS based on the number of employees associated with agencies. Each agency had an individual approach based on their environment, resources and size.

Large Size Agency

Process Overview

The process at the Large Agency started with the agency hiring a Chief Information Security Officer (CISO). The CISO was the impetus for the Information Security Policy Implementation. Apart from the pilot meetings, the Large Agency conducted regular weekly meetings to focus the efforts on the policy implementation work. They conducted daily touch points with respect to progress in the policy implementation and [Eliminate the use of this term or contact risk management.] roadblocks or challenges faced by individuals.

The Large Agency identified roles and responsibilities (via the Roles and Responsibilities Chart) to various individuals depending on the areas of specialization. Roles establish included a CISO, Assistant Executive Director, Chief Information Officer (CIO), Senior Information Security Officer, Security Operations Lead, Chief of Staff and Hiring Manager.

The agency developed the implementation plans based on the gaps identified as part of the gap analyses that were performed. The implementation plans were developed with the combined efforts of CISO, Assistant Executive Director, Senior Information Security Officer and Security Operations Lead. They identified long term and short term implementation plans; the latter being plans where the implementation lacked resources, professionals and/or budget. They highlighted the identified gaps in the implementation plans and incorporated those as part of the new budget request. The plans are to be revised with additional detail once the appropriate resources, professionals and/or budget have been approved or acquired.

The Large Agency has been focusing on their attempt to the change the work environment towards a more security centric culture for fast and efficient adoption and implementation of the policies. For this purpose, the agency employed has a couple different strategies such as security articles being published in the weekly newsletter, adopting security slogans (such as ‘Security First’) and security tips to start staff and board meeting to emphasis security as a primary foundation of the agency. The Large Agency also hired an IT Auditor to evaluate the existing IT process and procedures and to help the agency align the current policies and procedures with the statewide information security policies.

Medium Size Agency

Process Overview

The Medium Agency identified roles and responsibilities (via the Roles and Responsibilities Chart) to various individuals depending on the areas of proficiency. For a brief overview of the roles that were involved in the policy adoption and implementation work streams, roles included a Policy Champion, IT members, Asset Management Team, Division Directors, Procurement Services, Human Resources and Internal Audit Services. The Executive Director was identified as the main stakeholder in signing off the policies, procedures and standards that may likely be adopted during the policy adoption and implementation.

After the formation of the Policy Committee, the committee planned out basic timelines for the policy implementation process. The dates were set working backwards from the deadlines set by DIS. The Medium Agency's first step was to draft policies by the end of September 2014 to be reviewed to help understand potential budget implications. From September to January 21, 2015, the Medium Agency is planning to build out implementation plans for the DIS deadline. Starting in February 2015, the Medium Agency wanted to start rolling out policies or sections of policies that were ready for implementation until July 2016, the final compliance deadline. The Medium Agency has already started with remediation activities with the easier fixes such as access control forms, hiring procedures and procurement, among others.

The process at the Medium Agency started with the formation of Policy Committee and identification of the Policy Champion. The Policy Committee that led the policy adoption and implementation comprised of Policy Champion, Chief Information Officer (CIO), IT Manager, liaisons from department leads and members from the Internal Audit Team. The Policy Committees conducted weekly meetings; normally on Mondays (sometimes more frequently) to decide the course of action for the week and discuss the status of previous week. During these meetings, the tasks for the week were identified and roles and responsibilities for each of the individuals were set. The Medium Agency set an internal process called "Procedure Friday", where the agency may likely assign individuals with the task to draft procedures and forms with respect to a given policy on a weekly basis. The procedures that were due as part of "Procedure Friday" were decided during the weekly meetings on Monday based on the time availability of the resources that week. While drafting the policies and procedures, the Policy Committee reached out to the various divisions responsible for day to day operations for inputs, considerations, challenges and other thoughts as applicable.

Small Size Agency

Process Overview

The process at the Small Agency started with the identification of a Policy Champion. The Policy Champion led the policy adoption and implementation for the Small Agency with minor inputs from additional resources where applicable. Due to the size of the IT staff (4 in total), activities, meetings and documentation of templates was completed by the Policy Champion.

The Small Agency identified roles and responsibilities (via the Roles and Responsibilities Chart) to a few different individuals depending on the areas of specialization. For a brief overview of the roles that were involved in the policy adoption and implementation work streams, roles included a Policy Champion, IT Manager, Network Administrator, Database Administrator, Division of Operations Manager and the Executive Director was identified as the main stakeholder in signing off the policies, procedures and standards that could be adopted during the policy adoption and implementation.

One of the first tasks for the Small Agency was the data inventory and classification process. The agency assigned on lead to help manage the process and document responses from the various departments involved. They used one larger department of the agency as the pilot test group to see how effective the documentation could be captured and in the correct format that the agency wanted to utilize. Once the data inventory analysis is completed, the agency plans to move towards securing access rights to individuals based on the classification of data.

Given the size of the Small Agency, many meetings were scheduled on an ad-hoc basis to talk through the policy implementation process with managers and/or the Agency Director. In addition, there were monthly IT meetings to discuss the current environment which were going to be leverage to work on implementation plan strategies.

6.2 Detailed InfoSec Policies Overview

The following analysis helps to further breakdown some of the common misconceptions or assumptions of the State information security policies as well as typical challenges that an agency might face when it comes time for implementation of policy requirements. The guidance documented throughout this section was gathered through a combination of meetings and questions asked from various different inputs. Per policy, there are two main categorizes of guidance:

- ***Common Themes*** – For each policy, these common themes were summarized based upon the questions received from policy champions, agency directors or other inputs. The themes provide responses to help explain the reasoning behind the theme and how to work towards compliance. Regardless of the size of the agency, each policy has one or more common themes that could apply to their environment based on that policy's requirements.
- ***Typical Challenges*** – For each policy, there are associated challenges that have the potential to arise when attempting to grasp a particular process and align with the policy. These typical challenges were again taken from questions associated with the policy and give perspective for how to think through the potential solution. Each typical challenge has a brief explanation to provide background and a recommended solution that can help explain the thought process towards overcoming the gap. The solutions are not full-proof, but again, they help to provide the manner to which a policy deployment team can work towards overcoming that challenge in a simplified manner.

Asset Management Policy

Common Themes

Asset Management Is More Than Just Physical Assets

As identified during policy workshops and on-site meetings with agencies, a common misconception is that asset management is strictly focused on physical assets. As defined by the policy, agencies are required to identify, document and maintain four (4) different types of assets

- *Information assets:* databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information;
- *Software assets:* application software, system software, development tools and utilities;
- *Physical assets*: physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks); and
- *Services*: computing and communications services.

While assets can be maintained in separate inventories, the important aspect is to identify the truth of source where data can be centralized. The truth of source should be an inventory that is considered the master file which is ultimately used for asset reviews, audits, analysis and reconciliations. The more an agency can consolidate and condense assets in to a singular asset inventory (consistent of the 4 types of assets), the more efficient an agency can be in maintaining and complying with the asset management policy.

SCEIS (South Carolina Enterprise Information System) Used As Asset Management Solution

Building off of the previous common theme, on multiple occasions, agencies inquired as to whether SCEIS could be used as the truth of source to maintain asset types as the asset management solution to adhere to the State policy. Ultimately, the answer is No; agencies should not use SCEIS as the asset inventory solution. There are a couple reasons why SCEIS is not the correct solution. One, SCEIS was originally designed for the purpose of acting as a centralized HR, financial asset and payroll State solution. Second, agencies are required to enter physical assets that have a cost of $1,500 or more, but are not responsible for entering assets that do not meet the minimum threshold. In addition, agencies are not required to enter information, system or software assets in SCEIS, as required to be documented and maintained in the asset management policy. While SCEIS covers physical assets over $1,500, the system was not designed with the intention of becoming the inclusive, physical asset inventory for multiple agencies. Understanding that agencies are still required to enter physical assets meeting the threshold, within the implemented asset management policy, the agency should identify where the truth of

source (master file or system) for physical assets resides. In addition, there should be reconciliation steps (procedures) identified between the truth of source and SCEIS to correlate that the information is the same in both locations.

Typical Challenges

Challenges #1	Explanation
Lack of a centralized solution for asset inventory.	A common challenge among agencies was the lack of a centralized inventory of assets. Without a consolidated inventory, managing agency assets becomes a more difficult and segregated task.
Recommended Solution	
1. Utilize Excel spreadsheets or currently implemented software (e.g. Spiceworks), unless an asset management solution is utilized by the agency. 2. Assign responsibility to an individual who will be organizing the asset inventory. 3. Work closely with business process owners associated with each asset type (e.g. physical, information, software and services). 4. Document assets by four (4) asset types per the SC Asset Management Policy in one, consolidated 'truth of source' inventory. 5. Identify asset owners and establish a process for an asset management review on a periodic basis. 6. Work closely with DIS to determine if there is a recommended enterprise asset inventory solution coming on State contract.	

Challenge #2	Explanation
Not knowing what you have	One of the biggest issues facing agencies is the simple fact of not knowing what assets exist inside the agency. Without that understanding, the agency is at major risk for undetected breaches of data.
Recommended Solution	
1. Develop a systematic method of collecting data in a uniform manner. 2. Identify asset owners (by asset type) responsible for collecting data and organizing meetings with various areas or departments. 3. Work closely with business process owners associated with each asset type. 4. Combine collected asset data into one, consolidated 'truth of source' inventory. 5. Establish and configure an asset hierarchy. 6. Identify criticality of assets based on business requirements.	

Challenges #3	Explanation
Maintaining an asset inventory	While agencies are working to build their asset inventories, a main consideration post implementation will be how to update and maintain an up to date inventory list.

Recommended Solution

1. Identify asset owners (by asset type) responsible for maintaining their type of asset.
2. Implement a process that allows asset owners the opportunity to regularly update and monitor the asset inventory.
3. Provide appropriate access for maintaining asset inventory.
4. If applicable, coordinate management of agency assets with third-parties and define responsibilities of each party.
5. Establish an asset management review process that is conducted on a periodic basis that better fits the agency.
6. Implement a process to train, inform and provide guidance on asset management to asset owners and employees in the agency.

Data Protection and Privacy Policy

Common Themes

Classifying Assets – Only Information Type Assets

As mentioned in the Asset Management policy under the Security Impact Analysis section, agencies shall classify assets according to the State of South Carolina Data Classification Schema (e.g. public, internal use, confidential and restricted); however, not every type of the asset (e.g. physical, information, software and services) has to be classified. The sole type of assets that should be tracked and classified are ***information type assets*** (e.g. databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information). For example, an agency might issue laptops to employees. By issuing the laptop and setting up access, the agency should understand what type of data that employee has access to, including but not limited to, data files, SharePoint or similar file sharing services access, databases, applications, reporting capabilities, remote access connections, etc. Those access points should be classified according to the State schema and therefore, if the employee were to lose said laptop, the agency can efficiently tie the laptop to the employee (through the asset inventory), efficiently determine what access rights they had to agency applications, databases, etc. (through access request documentation), and determine the type of data and impact level (data classification exercise/inventory) one could gain access to outside of the agency protection. Based on that analysis, the agency could then determine in an accelerated manner how high the overall risk of data breaches and data loss is to the agency. At the end of the day, the data classification exercise is geared to identify the data that is used, produced and collected during daily business operations. A quick check agencies can use when trying to classify data is to always remember that one should classify the actual data (information asset) and not the device or service used to access said data. Those devices and services should only be documented and maintained as part of the asset inventory.

A Method of Classifying Data –Data Inventory Tool

To help an agency classify their internal data and align with the State data classification schema (e.g. public, internal use, confidential and restricted), a *Data Inventory Tool* was developed and published to the DIS website. The State of South Carolina established a *Data Classification Schema*, which provides the foundation for data classification efforts across the State. Classifying data according to its sensitivity level provides insight into how data should be handled and protected across an agency. The Data Inventory Tool is a Microsoft Excel spreadsheet which contains worksheets that guide a business process owner (e.g., program area/data owners) through performing a data inventory analysis. The Data Inventory Tool provides agencies with a standardized method to document and classify the data collected and processed by various agency systems. The tool is based on a system-level view of data sets within agency defined business processes. Data that is linked to a specific business process (e.g., HR data) is referred to as a "data set" for the purpose of this Inventory Tool. Throughout the data classification process, the tool contains worksheets that provide agencies with the ability to perform consistent data classification activities. Within the Data Inventory Tool, an agency can also find a copy of a Data Classification Decision Tree for guidance on how to properly classify Agency data. Business process owners are encouraged to use this decision tree in order to fully understand the process of classifying data. For further details on The Data Inventory Tool and supplemental procedures, instructions and templates, please refer to the *Resources* tab of the DIS website (http://dis.sc.gov/resources/Pages/default.aspx) under the *Tools* section.

Typical Challenges

Challenges #1	Explanation
Lack of data classification	The common challenge agencies are facing with respect to data protection and privacy policy is that agencies do not classify data within their environments. In addition, agencies did not have a method of producing a data classification inventory based on pre-existing templates.
Recommended Solution	
1. Complete the Data Protection and Privacy gap analysis to better understand the current environment of the agency and closer align to the State policy. 2. When applicable, participate in the Data Inventory tool training held or review materials presented. 3. Utilize the Data Inventory tool posted on the DIS website as the method to classify data. 4. Work closely with business process owners and IT asset owners to classify the data according to the State data classification schema. 5. Consult other agencies using similar types of data for additional support or to leverage commonalities.	

Challenges #2	Explanation
Lack of user education and awareness among agency employees for protecting data once classified	A major hurdle that agencies will face when implementing the data classification schema into daily business operations is employee knowledge with how to utilize, interact and protect data according to each level of the schema.

Recommended Solution

1. Publish and inform employees about the new State data classification schema.
2. Develop a data classification awareness training for users and contractors that handle agency data which should demonstrate the importance of each classification level and how they should interact with the data to protect the agency's security interests.
3. Consider developing email awareness training (or other significant daily function specific training) for how to specifically handle confidential or restricted data.

Challenges #3	Explanation
Lack of resources towards data sanitization procedures	Another challenge faced by agencies related to data protection and privacy is that they do not have sufficient resources or skill sets to help with data sanitization processes and procedures which can increase the risk of exposure to sensitive data.

Recommended Solution

1. Identify third-party entities to help with data disposal and data sanitization process.
2. Define the responsibilities for employees and third-parties who are involved the data disposal and data sanitization process.
3. Develop a service-level agreement, SLA, (or similar agreement such as a Memorandum of Understanding, MOU) for the agency that specifically identifies the responsibilities of each party and covers the proper security requirements from the policy.
4. Identify the type of data (e.g. especially confidential and restricted data) that constitutes sanitization and the level of details associated with each data type to better protect the agency from a risk of exposure.
5. Develop, document and implement data sanitization procedures for uniform compliance throughout the agency, uniquely identifying the roles and responsibilities associated internally versus those handled by a third-party vendor.

Challenges #4	Explanation
Lack of acceptable controls for data protection	One of the leading issues facing agencies is the lack of sufficient controls to protect data against vulnerabilities and potential losses of sensitive data.
Recommended Solution	
1. Utilize basic encryption methods (e.g., Public Key Encryption) and implement a secure communication channel to protect data in transit. 2. Utilize encrypted disk and flash memory drives for data at rest and data transfers. 3. Implement access controls based on the data classification exercise to restrict agency data to only those individuals who require access based on their daily job responsibilities.	

Access Control Policy

Common Themes

Lack of Accompanying Documentation (Process There – No documentation)

When working through the access control policy with agencies, the common theme recognized was the lack of documentation that was associated with existing processes and procedures (both compliant and non-compliant). As agencies worked through the gap analysis template associated with the Access Control policy, a majority of the gaps identified were related to missing or out of date documentation. In order for agencies to be in compliance with a particular security requirement from the policy, not only do the agencies need to have the process in place and operating effectively, but also the accompanying documentation to support the procedures associated with that process and the underlying forms and templates used in the execution of the process. This theme is applicable to each policy and it is important to keep in mind that a control is only as effective as the underlying documentation associated with security requirement.

Examples of the type of missing documentation associated with certain requirements included, but was not limited to, new and terminated user procedures, accompanying request forms for new access or removal of access, user access review procedures, evidence to suggest the existence that a review occurred, password control requirements, remote access forms, privileged account documentation, wireless access requirements and segregation of duties roles.

Minimum Password Requirements

One of the more common areas where agencies had questions based on difference s to the State policies was related to the password requirements documented in the Access Control policy. Agencies continually mentioned that their internal policy and application setting passwords are different or held to higher standards than those outlined in the policy. Ultimately, the policy highlights the *minimum* password requirements that agencies should implement to be compliant. Agencies have the flexibility to set stricter standards and requirements to better protect and secure internal data. The password requirements set the baseline compliance level and agencies should not go lower than the policy.

Legacy Systems

Trying to adapt legacy systems to the State information security policies requires research, coordination, flexibility and an understanding of overall risk. The age and technical capabilities of these systems may sometimes present difficulties in complying with the State information security policies. With that in mind, agencies should make a strong attempt to try and configure legacy systems to meet the policy requirements to lower the potential risk of data loss. After exhausting attempts to align the legacy systems to the policy, agencies may find that certain requirements are not capable of complying with the requirements. An example could be the password requirements of a legacy system. Based on the system configuration of the legacy system, when an administrator tries to change the password settings, it may prevent jobs from running in the background or lock users out of their daily job responsibilities. In these scenarios, agencies should utilize the 'exception process' once finalized by DIS. The exception process is an excellent example for how to handle legacy systems that have a hard time conforming to State policies and require special amended processes. Agencies are still recommended to analyze the greater risk of exposure based on that system and make adjustments where applicable, but if they feel the risk is acceptable based on the requirement, the exception process can be utilized.

Typical Challenges

Challenges #1	Explanation
Access level assignment and approval	Providing the applicable access to the desired users/employees is one of the biggest areas of improvement agencies can utilize to reduce the risk of data exposure. In addition, having a defined access request, assignment and approval process can better safeguard access to information system data.
Recommended Solution	
1. Implement a process for system access request and approval within the agency (both new hire and additional access requests). 2. Utilize the data inventory tool to identify critical business processes, critical systems and business/data owners. 3. Implement a Role Based Access Control (RBAC) framework. 4. Train employees/departments on the responsibilities of the system access request process 5. Designate appropriate managers whose responsibility is to assign and approve application/information system/data level access to employees, vendors, partners and third-parties. 6. Only allow system administrator grant access following documentation and authorization from a designated manager. 7. If applicable, assign read-only access to confidential or restricted data to those employees who need access to view data, but do not require rights to manipulate data.	

Challenges #2	Explanation
Managing access for transferred employees within Agency	A hard challenge faced by agencies is managing the access revisions of transferred (or terminated) employees. Lack of access revisions may allow unauthorized users to have access to resources or assets.

Recommended Solution

1. Establish process for access removal for the employee/contractor upon transfer, termination or end of contract connecting HR, IT and the hiring department manager.
2. Obtain required approvals from employee's manager to remove application/system access in a timely manner.
3. Obtain new access request documentation, including approvals, from the employee's new manager.
4. Determine if access removal for the former position is immediate and how it affects certain application/systems.
5. Stay in constant contact with the transferring employee or the accompanying managers to determine when access to old systems and rights are no longer applicable to their new job responsibilities.
6. If required, perform data wiping and sanitization on employee's equipment.

Challenges #3	Explanation
Managing file shares and shared drives	Another challenge that the agencies struggle with is access control on file shares and shared drives on the network.

Recommended Solution

1. Document the data inventory tool showcasing critical business processes, business process owners and critical data residing within applications, systems and files.
2. Scan the file shared drive and keep an inventory of sensitive data residing in that location (e.g. consider implementation of DIS's data discovery tool when available).
3. Determine whether data should remain on the shared drive.
4. Determine if access should be altered to restrict users and assign appropriate users and levels of access.
5. Provide awareness and training to employees for what can be uploaded and how to maintain proper levels of security around confidential or restricted data.

Challenges #4	Explanation
Controls over Remote Users	Agencies face challenges in controlling access of remote users, restricting remote users from the main network and logically separating or segmenting their access to better protect the agency from data exposure.

Recommended Solution

1. Establish remote access policies and procedures to govern user rights.
2. Provide guidance to managers and employees on remote access requirements.
3. Deploy tools (i.e. VPN using 2FA) to protect the inbound and outbound flow of data.
4. Use logical separation to restrict access of remote users in the agency network.
5. Train personnel on proper usage of remote access to the agency's network and information systems (e.g. avoid saving critical information locally [i.e. personal PC], unless remotely accessing the desktop).
6. Limit remote access to users based on business need.

Information System Acquisition, Development and Maintenance Policy

Common Themes

Defining Requirements for the SDLC Process

A major component from this policy is the creation of a System Development Life Cycle (SDLC) process, more specifically, change management procedures. The change management procedures govern procedures from the change request through testing, approvals and confirmation that the change was effective, including supporting documentation. The process itself can be very cumbersome dependent on the nature of the change and the effect the change has on employees. In addition, parts of the change management process may be outsourced to third-parties, such as the Division of Technology Operations (DTO). The change process might vary from system to system based on type of application, years in service and configuration. Based on these factors, it is important to define the requirements for each party and procedures that apply to the agency versus third-parties operating on behalf of the agency. For example, as an agency, you may define in the policy that changes that effect less than 20 total users (less than 10%) of employees go through a condensed version of the change control process whereas changes that effect 20 or more users follow the full change management process. Another example could be that for those changes that deal with confidential and restricted data, added layers or testing and approval are required to further analyze that the change addresses business circumstances and is thoroughly vetted before implementation to users. When working with third-parties, an agency may identify that they are responsible for initiating the change, testing, approval and post-implementation validation, but the third-party is responsible for developing, initially testing, safeguarding the version control and migrating the change to production. If the process is outsourced (to DTO for example), the agency should utilize Service Level Agreements (SLA), Memorandum of Understanding (MOU) or other subsequent agreements to Ultimately, an agency should understand each phase of the change management process and document the process accordingly in the policy and/or procedure(s). When documenting the change management process, be sure to define requirements that apply to certain situations, types of systems, change types, etc., to help the agency better navigate change management. The agency should weigh the overall risk of changes, the data affected, operational efficiency of the change and severity of the change when documenting the procedures to better align itself for an effective change management process.

Protecting 'State Interests' Through Procurement

During agency meetings, one particular policy requirement presented an open-ended interpretation that was later clarified by the DIS office. The policy requirement was as follows, "[Agency] shall ensure that the State's interests have been protected and enforced in all IT procurement contracts. Further questions were raised by policy champions to clarify if this bullet could be translated to me that third-parties should follow the same policy requirements as the agency, such as the SDLC process. The answer provided by DIS was as follows, "Yes, the Agency needs to require third-parties to follow the same standards as outlined in the State information security policies. Within the Service Level Agreement (SLA) or other contract, the requirements of the State's interest should be represented accordingly." Agencies, whether through internal operations or outsourced processes, need to have protections in place to safeguard data in accordance with the State information security policies, thus protecting State's interests. Based on the defined processes and procedures, agencies should work closely with third-parties to outline policy requirements in SLAs, MOUs and other contracts to appropriately protect themselves from the risk of data exposure.

Typical Challenges

Challenges #1	Explanation
Secure Coding Practices	Hiring/finding skilled codes who utilize secure coding practices for development of application/software is one of the biggest challenges faced by agencies. Also, when development is done by a third party, agencies find it hard to analyze that secure coding practices are used
Recommended Solution	
1. While recruiting application developers, explicitly test for knowledge of secure coding practices. 2. Develop training curriculum with respect to secure coding practices based on references from OWASP, CERT and other resources. 3. For existing staff/developers, provide trainings based on the developed curriculum, highlighting the need of the same. 4. During the testing phase, test for security flaws through code scanning, code reviews and/or security testing (such as penetration testing or vulnerability assessments). 5. For agencies that utilize third parties for developing their applications/software, perform security assessment or audits to assess the use of these practices.	

Challenges #2	Explanation
Lack of a structured communications process	It is important that the communication process during the SDLC process. It is important that the requirements and feedback of the end user to the development community.

Recommended Solution

1. Establish a structured communication process to solicit inputs from end users.
2. Develop documentation (e.g. change request forms) to help capture and streamline communication throughout the SLDC process.
3. Encourage period ‘debriefs’ between the developer community and the end user.

Challenges #3	Explanation
Emergency Changes	While doing emergency changes to production systems, agencies often bypass the change management process and incorporate the changes. If the emergency change process is not properly documented for changes to the normal change management process, important attributes can be overlooked and potentially inappropriate changes are migrated to production.

Recommended Solution

1. Determine what type of changes could be classified as emergency changes.
2. Develop an emergency change management process that specifically identifies differences from the normal change management process.
3. Define how documentation will be maintained (e.g. during emergency changes, it is common that documentation comes after the change is migrated to production).
4. Such changes should be reviewed and approved by a member of the security team (i.e., information security officer or equivalent) and approved by an authorized individual (i.e., IT director or equivalent).
5. Determine whether approvals come before or after the change is migrated.
6. Validate that documentation is captured and saved once change process is completed.

Threat and Vulnerability Policy

Common Themes

Enhancement of Patch Management Processes

Over the course of the risk assessment workstream performed with multiple agencies over the course of the past year, a more common improvement area for the State revolved around patch management. Through analysis of State environments, patch management processes and improvement left the State vulnerability to potential data loss. Agencies should spend time reviewing this section (1.3) of the T&VM policy and align their internal processes or work with third-parties (e.g. DTO) to identify and adapt controls and processes that will provide appropriate protection against threats which could adversely affect the security of the information system or data entrusted on the information system. Agencies should continue to work and establish requirements such as defining patch schedules, research to identify when better methods to discover when patches are available, enhance testing procedures, establish measures to identify, report and correct approaches information security flaws and implement more capable patch management solutions. Agencies should consider deploying a centralized patch management solution (e.g. recommend participating in the DIS State offered solution Secunia Patch Management). In addition, keep an inventory of specific technology used within the agency and have dedicated resource to keep track of new patches and security vulnerabilities. From the inventory of technology, document the end of life products and technologies (e.g. such as Windows XP) for awareness when patches are no longer available to remain secure. To help from a solution standpoint, there are currently two patch management solutions on state contract: Secunia CSI and IBM/Tivoli Endpoint Manager. In addition, DTO is currently working towards rolling out a new solution, Secunia CSI. Over the past couple months, DTO has been working diligently to test the solution during the pilot phase and are on schedule for State wide deployment later this year.

Incident Handling Procedures

In the event of the threat of data breaches or tangible data loss, incident response plans become a vital exercise for an agency. The incident response plan (IRP) can be the difference between minor data loss with little to no interruption in daily procedures and potential loss of reputation and non-recoverable sensitive data. As the policy states, there are multiple areas that make up the incident handling procedures. One of the more important features of the IRP is having to communication responsibilities, channels and reporting structure vetted and in place for employees and management. Incident response detection, analysis, containment, eradication and recovery are only possible if the chain of command is in place and responsibilities are defined to efficiently assess the magnitude of an incident within the agency. While it is imperative to have the incident response plan documented, the accompanying department or area procedures are just as important as the overall plan. Employees should be aware of their responsibilities and trained on the requirements that apply to the actions needed to efficiently understand and remove the incident from becoming serious and damaging. Testing of the incident response process is to be tested on an annual basis and an important but sometimes overlooked detail associated with the testing is the improvements that should be added based on lessons learned. Lessons learned can provide valuable insight to missed steps, improper methods of communication or lack of training, which should be worked back in the IRP to improve the process. Implementation of an incident management framework will work to secure the information system against potential vulnerabilities and threats.

Typical Challenges

Challenges #1	Explanation
Identification of false positives	One of the challenges that the agencies are facing is identification of false positives in terms of incidents and vulnerabilities such as fake malware infection alerts from the SIEM or inexistent vulnerability identified by the vulnerability assessment tool etc. False positive may lead to waste of efforts and resources in addressing nonexistent issues.
Recommended Solution	
1. Maintain a process to document any identified incidents and vulnerabilities within the agency. 2. Document and maintain a list of known false positives that were identified. 3. Cross reference the new incidents and vulnerabilities with the identified list of incidents and vulnerabilities within the agency and known false positive. 4. Have a plan to socialize the list with the required individuals based on job responsibilities.	

Challenges #2	Explanation
Lack of documented and implemented incident response procedures	Although a lot of agencies have incidence response procedures, a lot of agencies face challenge in having fully documented and implemented incident response procedures.

Recommended Solution

1. Establish an incident response team comprising of main individuals from the agency.
2. Develop and document an incident response processes and procedures which comprises of (at the minimum)
    - Conducting initial assessment of the incident
    - Developing initial response to the incident
    - Collecting forensic evidence
    - Implementing temporary fix
    - Developing and distributing communications (i.e., internal and external)
    - Implementing permanent fix
    - Determining financial impact on operations
    - Documenting lessons learned
3. Analyze and improve the existing incident response processes and procedures based on the lessons learned from previous incidents.

Challenges #3	Explanation
Understanding zero day vulnerabilities and threats	Understanding zero day vulnerabilities and threats is another challenge faced by agencies. Zero day threat is an attack that exploits a previously unknown vulnerability in a computer application, one that developers have not had time to address and patch and hence cannot be protected against.

Recommended Solution

For security personnel in the agency:

1. Collaborate with SC-ISAC and DIS to get a good understanding of the zero day vulnerabilities, and potential attack vectors.
2. Keep up to date with technology vulnerabilities from open blogs, security journals etc.
3. Acquire certifications such as SANS GPEN, CEH to get a better understanding of the dark web and acquire source materials to gain access to zero day exploits.
4. Attend security conferences (such as Blackhat, Cyberlympics etc.) to get a better understanding of the latest security practices and threats.
5. Perform threat intelligence monitoring through third party vendors.

For non-security personnel in the agency:

6. Keep employees up-to-date through an agency security newsletter or magazine or weekly meeting.

Challenges #4	Explanation
Employee awareness	Agencies struggle with creating user awareness of various threat vectors that organizations face on a day to day basis
Recommended Solution	
1. Provide training and awareness of the various threat vectors in the industry and an understanding of how to react in responsible ways. 2. Provision employees with basic trainings such as the ones offered by SANS. 3. Collaborate with DIS, DT and other agencies to enhance employee awareness. 4. Stay up to date with threats through research and continual monitoring.	

Business Continuity Management Policy

Common Themes

Business Continuity Management Includes More Than Disaster Recovery

Based on experience, a common error companies and agencies continually make is mistaking Business Continuity Management (BCM) as solely an Information Technology Disaster Recovery (ITDR) exercise. BCM and ITDR, while related with dependencies, require separate considerations and planning in order to fully implement a full and effective Business Continuity Management plan. BCM deals with the management of people, resources and communication while the ITDR covers the management of technology, backups and recovery. The first half of BCM is just an important, if not more important, than the latter DR piece as without the proper planning for communications and user management, an agency could fail to recover from an incident in a manageable timeframe. The counter argument is that without the effective recovery of applications, databases and systems, the agency cannot perform its mission and main business functions. While true, a huge component of DR is dependent on communication channels, chain of command, resource availability and employee roles and responsibilities, the components involved with proper BCM planning. Employees need to know what to do in the event of an incident or disaster and without the supporting structure identified when developing a BCM, the opportunity for further disruption and negative consequences is significantly increased for the agency. BCM planning is a main driver for the effective implementation of the overall Business Continuity Management and Disaster Recovery plan.

Business Impact Analysis (BIA) before Business Continuity Management (BCM)

Throughout the course of the risk assessment process performed on the statewide agencies over the past 18 months, one domain that was consistently flagged as a high risk area for agencies was Business Continuity Management (BCM). The main reason for the higher risk ranking was due to the fact that agencies had not conducted a Business Impact Analysis (BIA) first in order to align their BCM and IT Disaster Recovery (ITDR) plans adequately. In order to implement an effective BCM plan, the first step for an agency is to understand the full impact a disaster might influence on the agency's mission, people and supporting infrastructure. A BIA helps an agency predict the consequences of disruption to business functions, processes and gathers information needed to develop recovery strategies. During the BIA an agency will identify critical business processes, applications and information systems that are critical to continue the mission of the agency. Based on the results of the BIA, Agencies can define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). RTOs and RPOs are imperative to BCM and DR planning, as these define the tolerance levels to recover potential loss of data and/or loss of service and not disrupt daily business operations in a negative manner. In addition, the BIA also helps identify business dependencies and operational processes which are vulnerable during the time of a disruption. Another benefit of completing the BIA is that an agency will also identify roles and responsibilities that are applicable for DR planning and recovery activities.

Typical Challenges

Challenges #1	Explanation
Lack of Disaster Recovery (DR) testing	Agencies in general do not perform regular DR testing and exercises. Regular exercises help determine flaws in the existing DR plan and help improve the process.
Recommended Solution	
1. Conduct table top BC and DR exercises. 2. Conduct dry runs (or practice runs) in testing information systems to study where the effects of a possible failure are intentionally mitigated and update the existing DR plan based on the results from the table top BC DR exercise and the dry runs. 3. Have a third party conduct a ITDR assessment on the agency to know the effectiveness of the DR processes and procedures and update the update the existing DR plan, processes and procedures based in the results from the third party assessment.	

Challenges #2	Explanation
Lack of Business Impact Analysis (BIA) and define business critical functions	Without first conducting a BIA, an agency cannot begin to understand critical business functions as well as define roles and responsibilities for individuals and define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
Recommended Solution	
1. Develop or utilize a BIA template (potential to work closely with DIS for BIA template). 2. Establish a list of the Agency's critical information systems (e.g., through a BIA). 3. Establish acceptable tolerance levels for critical applications. 4. Define roles and responsibilities for employees related to BCM and DR processes. 5. Define RTOs and RPOs.	

IT Risk Strategy Policy

Common Themes

Metrics That Matter

Metrics are only as effective as the change that they can help drive in a company, organization or agency. The establishment of metrics within an agency helps to evaluate the adoption of security controls and policies/procedures and measure the effectiveness of the information security program. When designing metrics, an agency should consider first understand their current environment and what raw data is readily available for metrics and analytics. Data elements can come from many different sources within the agency. The goal is to design the metrics in a meaningful manner. As described on slide 11 of the IT Risk Strategy presentation, an effective way to drive meaningful metrics is by using the S.M.A.R.T. (specific, measurable, actionable, realistic, and timely) methodology. The driver behind S.M.A.R.T. metrics is that they yield corrective actions rather than the establishment of metrics that seem useful but when broken down, have no source of failure. Metrics should tie to an area, department, individuals or other main source that can have actionable results such as the retraining of employees, adjustments to processes, increases or decreases in documentation or other correction action. Another aspect to metrics is that each one should be shareable, reportable and easy to understand and digest. The number of metrics established is dependent on the environment of an agency. A suggestion could be to start small with the establishment of metrics that are easy to track, easy to obtain data points and are able to help dictate the adoption of security controls, policies/procedures and can measure the overall information security program. Consider building metrics that are for different lengths of time. For instance, the agency could track which policies have been implemented over the next two years towards the compliance date of July 1, 2016. That metric has a defined period of time and once met, will be removed from the implementation plan. Another example could be a metric established around the number of open exceptions to policy requirements. Again tracked through the compliance date, as policies and standards evolve not only within the State, but in the greater information security environment, this metric will be a constant throughout the existence of the agency and can help align the agency to better practices. Ultimately, the fundamental point of metrics is to avoid establishing metrics just to have metrics, but rather to have metrics that help motivate the agency to better align themselves to their overall mission.

Lack of Interagency MOUs

Throughout the State, a common missing element is the lack of or out of date Memorandums of Understandings (MOUs) between various agencies sharing data. Various agencies have their data hosted, shared or utilized by other State agencies in some capacity and take SLAs or MOUs for granted under the pretext that they protected in the event of data loss. Just because other State agencies are compliant with the same security requirements based on State, Federal and other subsequent laws and regulations, does not mean they are properly covered, especially without a signed and updated MOU/SLA. It is up to the individual agencies to protect their own data even if its managed, used, hosted or transmitted through another agencies. The MOUs and SLAs play a very important role in helping the agencies protect their individual data. Agencies are advised the deal with other agencies with the same scrutiny as a third party. While dealing with other agencies, each agency has to have a full MOU or SLA that specifies the requirements that have to be met while a third party (be it another agency or an actual third party) hosts/stores, handles, processes or transmits agency data. As agencies are moving towards the same set of policies, understanding of how to protect data should be similar across agencies and therefore, MOUs and SLAs could be similar in nature between agencies. The important aspect is that agencies should have MOUs/SLAs in place as protections to prevent data loss.

Typical Challenges

Challenges #1	Explanation
Data sharing with third-parties	Agencies are having difficulty controlling and knowing what agency data is being shared with third-parties. This an important step in evaluating third party risk to the agency.
Recommended Solution	
1. Use and complete the data inventory tool to help identify the data that being externally communicated to third-parties. 2. Review existing SLA (or ISA) agreements with third-parties. 3. Align missing State requirements to the existing SLA (or ISA) or establish new agreements with third-parties to maintain data protections.	

Challenges #2	Explanation
Controlling third party vendor	Another challenge that is currently faced by agency is controlling third party vendors in the IT environment. Agencies typically find it difficult to limit the access of third party vendors who enter the IT infrastructure through, VPNs or physical access and also the risk they bring to the agency by being on the agency network.
Recommended Solution	
1. Establish clauses and acceptable use polices for the use of Agency data/assets by vendors into the third party contract (SLA). 2. Govern the level of control for the vendor/contractor access point (such as restricting use to specific locations, utilizing VPN, etc.). 3. Analyze and oversee that vendor devices are patched and have antivirus to better protect the Agency data. 4. Control vendor access to information systems and make sure they are strictly regulated (e.g. to specific servers or subnet as opposed generic access or through the use of VDIs [Virtual Desktop Infrastructure]).	

Mobile Security Policy

Common Themes

BYOD (Bring Your Own Device) Policy Enabled With Proper Protections

Mobile device management is one of the more complex elements of the State information security framework. In addition, mobile devices are one area where many employees, whether in an IT department or other area, can relate as society has gravitated to the convenience of mobile devices (e.g. cell phones, tablets, laptops, etc.). For agencies, management and IT have allowed employees to connect and use personal laptops, iPads and mobile phones to handle business emails and other functions without necessarily understanding the repercussions of what might happen to agency data. Ultimately, a BYOD policy is not explicitly prohibited by the Mobile Security Policy. Each agency has to make a determination whether it can adequately protect business data on user devices. In order to protect the business data, an agency has to implement protections that lower the risk of potential data loss through three methods. First the agency should implement a policy (e.g. the Mobile Security Policy) to govern users and their responsibilities. This includes documentation of subsequent processes and procedures associated with the policy. The implementation of the policy should be accompanied by policy awareness and training, the second method. Awareness and training for employees is vital to effective implementing mobile device management. Employees should understand their responsibilities, how to protect data, what to do in the event of device loss and other processes. The final method is to have the technical means and solutions in place to protect mobile devices and potential data loss. Through the implementation of a MDM (mobile device management) solution, encryption methods, downloading and technical restrictions, usage restrictions and other means, an agency should feel that they have the proper technical means in place before allowing the use of a BYOD policy. BYOD can be done effectively, but an agency should take the required technical precautions and adhere to the restrictions of the Mobile Security Policy.

Typical Challenges

Challenges #1	Explanation
Control of mobile devices	One of the biggest challenges that the agencies are facing is the fact that the agencies are unable to control the mobile devices in their IT environment.
Recommended Solution	
1. Implementation of a Mobile Device Management (MDM) solution to mobile device handling agency data including email. 2. Use of agency issued devices only as opposed to BYOD (Bring Your Own Device). 3. Restriction on the device type or model or operating system (such as restricting agency devices to iOS as opposed to generic systems). 4. Security awareness and training for employees on use of mobile devices.	

Challenges #2	Explanation
Misuse of agency devices	Another challenge that the agencies are facing is with respect to misuse of agency devices. Agencies are finding it a challenge to control the devices and the data that resides on the devices.
Recommended Solution	
1. Security awareness and training for employees. 2. Use of MDM with Data Loss Prevention (DLP) capabilities to detect misuse or loss of data from devices. 3. Sandboxing of agency applications and agency data present in mobile devices.	

Challenges #3	Explanation
Control of removable media	Agencies find it difficult to control removable media such as USB drives, CDs, DVDs etc. in their IT environment. It is imperative that the agencies have better control over these removable media devices to reduce the risk of sensitive data exposure.
Recommended Solution	
1. Disable the use portable/removable media devices on agency endpoints and servers 2. Promote the use of encrypted disk drives such as encrypted USB keys, CDs, DVDs etc. 3. Use of whole/full disk encryption on the agency portable devices such as laptops, mobile devices etc. (dependent on data classification levels)	

Challenges #4	Explanation
Webmail control	Another challenge that the agencies are facing with respect to control of mobile devices is that agencies are not adequately prepared when employees use their personal mobile devices to access the web outlook interface. Since web outlook enables personnel to open and download attachments, the agency data may be put at risk by downloading the same to personal devices owned by agency personnel. This is challenge is not only applicable to mobile devices but also applicable to personal desktops or laptop devices.
Recommended Solution	
1. Security awareness and training for employees on secure use of agency information. Emphasize on, not using personal devices to access agency related information. 2. Update the acceptable use policy of the agency, explicitly highlighting the prohibiting the use of personal devices to access agency data (also referencing the use of web outlook). Also highlight the penalties applicable, if found non-compliant. 3. Have employees and contractors (or third party vendor) sign or acknowledge the updated acceptable use policy and follow up with actions and penalties on an event of non-compliance. 4. Configure the Outlook Web Application (OWA) to disallow direct file access/attachments to restrict attachment opening via OWA.	

HR & Security Awareness Policy

Common Themes

Human Resources as a Foundation of Information Technology

Per conversations with agencies, one common observation was the disconnection between the human resources (HR) and information technology (IT) departments. HR plays an integral part in helping IT manage resources throughout a user's career. The two departments should maintain an open and clear line of communication in order to effective handle access management, training & policy awareness coordination, business continuity management, security operations and various other functions. As mentioned, access control for the provisioning of users is heavily dependent upon notification from the HR department. For new hire access, HR is one of the first departments to know of the new employee, either through the hiring process or by notification from the associated manager. Through new hire request forms, including proper approval, HR should notify the IT department of the new hire so that IT can work with the associated manager to provision the correct access based on job responsibilities in a timely manner. For terminated user or transferred employee access, the notification between HR and IT becomes even more important. Upon the termination or transfer, HR should promptly notify IT of the situation in order for IT to remove access to information systems in a timely manner to prevent inappropriate access exploitations by a user. Without that notification to IT, access can be left open leaving potential vulnerabilities for days, weeks or even months. While there are many further examples, the point remains that HR should remain connected with IT rather than staying separate from responsibilities. When HR and IT work together, information security requirements are further strengthened to help support compliance with the policies.

Training Based on Job Functions

A main aspect of the HR & Security Awareness Policy is at the end of the following requirement (in italics), "[Agency] shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to, contractors and third party users, *as relevant for their job function*." When it comes to implementation of processes and procedures, role-based security training is the correct method for agencies. Rather than teaching each employee about specific requirement of the policies, agencies should tailor the message based on roles, responsibilities and the overall function of the employee. For instance, a manager in a finance department does not need to know how access to systems is configured, however, they do need to know how to initiate the new employee process, fill out subsequent access request form and approve access to the systems, where appropriate. Another example for the same manager could be that he or she does not need to know how the data disposal process works, but they may need to be trained on the termination process to let IT know the employee is no longer apart of the agency. Employees may likely not need to know how data is classified during the data inventory tool, but employees need to be trained on data classification and their responsibilities for sending, receiving, transferring, printing and using confidential and restricted data versus public and internal use data. While there are countless other examples, employees should be aware of their new responsibilities from implemented processes and have access to review the policy when needed. The important lesson is that training (see section 3.4 Policy InfoSec awareness for different methods) should be tailored based on the job functions of the employee.

Typical Challenges

Challenges #1	Explanation
Changing the security culture	Changing the security culture is one of the more important aspects on implementing an effective information security program and it is also one of the more common areas agencies struggle with. Agencies and agency employees have often preferred convenience over security in the past and have exposed themselves to a wide array of risks. Agencies should change the culture as a whole so that a security centric culture is developed within the agency to minimize the risks for the agency.
Recommended Solution	
1. Provide generic security awareness training to employees, security seminars and conferences to change the security culture. 2. Develop multiple methods used to drive the same security topic (e.g. trainings, posters, slogans, newsletters, email, etc.). 3. Provide tangible examples for employees to relate new security requirements to daily tasks (e.g. hard-paper with PII/FTI data). 4. Continually enforce the importance of security awareness.	

Challenges #2	Explanation
Role based security training	A very common challenge that is being faced by agencies is to provide role based security training. Agencies find it difficult to provide security training to different employees, contractors and third-parties security training as required by their roles and responsibilities and end up providing generic security training to employees. It is important to provide role based security trainings to employees, contractors and third-parties according to their roles as some of them may be handling more sensitive information than others and require stricter security knowledge than others.

Recommended Solution

1. Provide generic security training to employees (like SANS trainings etc.).
2. Provide on-the-job trainings and role-specific trainings to the employees based on the role of the employee during recruitment, promotion or transfer.
3. Certification requirements based on the level or designation of the employee (like CISSP for ISO, CCNA for Network Managers etc.).
4. Provide job specific trainings to third party vendors and contractors and provide them access only after effective completion of these training courses.

Physical & Environmental Security Policy

Common Themes

Securing Data Center for Small and Medium Agencies

The physical and environmental security policy talks about security controls that have to be implemented to secure the agency datacenters, server rooms etc. Agencies face substantial challenge in incorporating the security controls as they do not have a designated datacenter and/or lack the funding to implement the controls. This is a pervasive issue among the small and medium agencies. Quite often, agencies end up spending more on controls and datacenter security than what the datacenter is worth. Hence, agencies are advised to perform a cost based evaluation before implementing physical and environmental controls for datacenters. In such an event, the smaller agencies are advised to use shared services offered by DT/DIS (or other third party services) to host their data. This helps reduce the financial burden on smaller agencies to comply with the requirements stated in the policy. However, agencies who do utilize shared services offered by DT/DIS (or other third party), have to have detailed and specific SLA in place with the concerned parties addressing requirements that need to be met prior to hosting their data.

Typical Challenges

Challenges #1	Explanation
Securing the datacenter	Agencies have a hard time locking down access and providing environmental protections controls for their datacenters, especially when they use third-parties host their data centers as they have less control over them.
Recommended Solution	
1. Restrict physical access of employees or visitors to the Datacenter. 2. Provide access based on need to know basis (as opposed to generic access). 3. Segregate the Datacenter into different portions depending up on the devices and sensitivity of the data present on them and provide access based on that (stricter access to devices and assets hosting highly sensitive data). 4. Implement protection mechanisms for fire protection, humidity and temperature controls as well as emergency power back up for the certain data center. 5. For agencies leveraging third party datacenters, have Physical & Environmental Security as part of the SLA with the third party and conduct risk assessments for compliance Perform data center visits to assess the physical and environmental security controls.	

Challenges #2	Explanation
Securing data outside the data center	Agencies often focus only on the physical and environmental controls on the data center. It is important to have the same controls for assets (both physical and electronic) outside the datacenter; like servers, workstations, hard copies of documents etc.
Recommended Solution	
1. Restrict physical access of employees to the servers and assets by having then behind closed doors with proper access control mechanism. 2. Provide access based on need to know basis (as opposed to generic access). 3. Implement protection mechanisms for fire protection, humidity and temperature controls as well as emergency power back up in the form of a power invertor or UPS. 4. Implement a clean desk policy to prevent hard copies of documents floating around near workspaces.	

7 Appendix G – Information Security Plan Development Guidelines (from DIS)

Information Security Plan Development Guidelines

for all South Carolina state agencies

version 1.0

issued: 03-Jun-2014

effective: 03-Jun-2014

Purpose

This document is intended to provide guidance for any South Carolina state government agency in developing its Information Security Plan. An agency's Information Security Plan is the collection of documents it uses to demonstrate its compliance with the South Carolina Information Security Program, which is documented on the DIS website: http://dis.sc.gov/policy

Definitions

Within the scope of this document, the following terms are used as defined here:

agency – refers to all South Carolina state agencies, institutions, departments, divisions, boards, commissions, and authorities

Executive Procedure

The executive director of an agency plays a vital role in the development of the agency's Information Security Plan, empowering staff delegates with the authority to act decisively, and providing the resources necessary to design and implement the Plan.

1. The **agency director** should communicate to the agency's senior management the agency's commitment to and priority for development of its Information Security Plan.
2. The **agency director** should review the steps outlined in the Management Procedure below, then designate and charge appropriate members of senior management with the responsibility and authority to perform those steps.
3. The **agency director** should require periodic progress reports on the development of the agency's Information Security Plan.

Management Procedure

The members of management within an agency should ensure that agency staff follows the processes outlined in this document, should report progress to executive leadership, and should provide or escalate resource needs.

1. **Agency management** should review the Technical Procedure below, as well as the Roles and Responsibilities Chart published on the DIS web page: http://dis.sc.gov/resources
2. **Agency management** should then designate and charge appropriate staff members with the responsibility and authority to perform the associated tasks.
3. **Agency management** should require periodic progress reports on the task assignments.

Technical Procedure

The Policy Champion is the lead staff member, charged with coordinating the following processes outlined below. Ideally the Policy Champion should have Project Management skills, in order to organize and manage actions of the members of staff who make up the Policy Deployment Team.

1. The **Policy Champion** should review and become familiar with all policy documents published on the DIS website at: http://dis.sc.gov/policy
   This familiarity will benefit other team members in coordination of efforts across all policy domains.
2. The **Policy Deployment Team Members charged with "Asset Management"** should review and perform the activities required by the Asset Management policy document published on the DIS website at: http://dis.sc.gov/policy
   Document assets using the Data Classification and Data Inventory tools published on the DIS website at: http://dis.sc.gov/resources
3. All other **Policy Deployment Team Members** should review their respective policies as published on the DIS website at: http://dis.sc.gov/policy
   Compare policies to existing agency processes and documentation, and perform gap analyses using the Gap Analysis tools published on the DIS website at: http://dis.sc.gov/resources
   Determine needed remediation for gaps using the Policy Implementation Plan of Action tool published on the DIS website at: http://dis.sc.gov/resources

Information Security Plan – Master Document

The Policy Champion should ensure that all document products of this process are secured in such a way that they are only accessible to agency staff members. In addition to the documents described in the above procedures, an Information Security Plan master document should be created, including the following elements:

1. A reference to the state Information Security Program, including URL (http://dis.sc.gov/policy)
2. A list of all documents created in the procedures above, including location(s) where master copies are kept.
3. A list of all relevant agency policies, procedures, and other documents that were reviewed, modified, or created during the procedures above, including location(s) where master copies are kept.