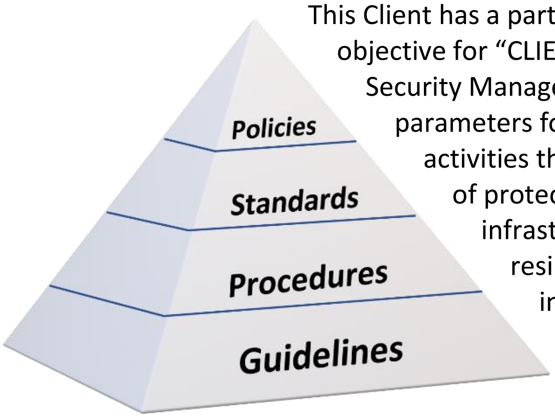
DREW
Blandford-Williams
GRC
cybersecurity consulting services

“Client” ISMS
Library ASSESSMENT

“CLIENT” ISMS Library Assessment

Summary



This Client has a partially established library of security policies and procedures. An objective for “CLIENT” to consider would be to formally establish an Information Security Management System (ISMS), which will provide the fundamental parameters for how “CLIENT” secures its data, its operations and any related activities that may pose a risk to confidentiality, integrity, and availability of protected information. Adopting an ISMS throughout the “CLIENT” infrastructure also targets the improvement of the company’s resilience to cyberattacks, and reduce the costs associated with information security throughout the “CLIENT” operating environment.

Structure

An ISMS is a systematic approach that impacts those processes, technologies and resources that help protect and manage CLIENT’s information through effective risk management. The structure used to establish an ISMS is based on the GRC parameters defined by ISO 27001. This international standard provides the baseline parameters for a best-practice ISMS, which may then be modified to align with “CLIENT” expectations and operational requirements. As there are more than 40 individual policies and associated modules within the ISO structure, some modules may not apply to the “CLIENT” operating environment. Moreover, ISMS content is somewhat segregated into three categories, as defined in the following table, although the activities defined within the ISMS may at times and in some business cases, overlap into other categories.

Policies	Policies represent the highest level of structure within the Information Security Management System hierarchy. These formal, high-level statements are aligned with the company’s goals, mission objectives and core ideology, and include specific directives on acceptable actions on behalf of a specific issue or topic. In short, a “Policy” is a statement of intent.
Standards	Standards represent the body of mandatory actions or rules necessary to support and validate a specific policy. Standards are fixed rules that achieve the intent stated in a policy. Data protection standards, for example, provide actionable controls (almost a checklist) to be implemented to protect data and subsequently comply with stated laws. The bulk of the ISMS documentation is comprised of Standards.
Procedures	Procedures describe the process to achieve a consistent goal or outcome (i.e., who is responsible for which tasks, when such tasks are performed, and requiring to fall under a specific criteria). Procedures are the implementation activities associated with all policies, standards, and guidelines.

Guidelines	Guidelines are general statements, recommendations or administrative instructions designed to achieve the policy's objectives by providing a procedural implementation framework. Guidelines should be reviewed/audited on a regular basis (recommended semi-annually), as they may change on a regular basis, based on the business environment within the "CLIENT" business environment.

ISMS Library (***Current "CLIENT" Status***)

	Policy Designation	Title	Type	Description	Status / Recommendation
1.	CLIENTP01-SPF	**CLIENT Global Information Security Policy Framework**	Framework	Purpose: Establish a framework for the development and maintenance of CLIENT's information security policies, standards, procedures, and guidelines and define the process for assessing and tracking non-compliance with policies, standards, and procedures.	Not Formally Defined although may be partially outlined by NIST or ISO standards
2.	CLIENTS01-BCS	**Business Continuity Standard**	Standard	This standard provides guidance to ensure critical business functions are promptly recovered and available to authorized users in the event of a major business interruption or disaster.	Not Formally Defined
3.	CLIENTS02-BRS	**Info Asset Backup and Retention Standard**	Standard	This standard protects the confidentiality, integrity, and availability of "CLIENT" data and electronic assets (including pii) by establishing baseline parameters for data handling.	Not Formally Defined as stated but referenced in "Back-up Retention policy" (Line #56).
4.	CLIENTS03-SDS	**SDLC Standard**	Standard	This standard ensures that security requirements for the confidentiality, integrity, and availability of the Company's information are included as an integral part of the Company's system acquisition, system development, and maintenance lifecycle process (SDLC).	Not Formally Defined
5.	CLIENTP03-CHP	**Change Management Policy**	Policy	Requirements and guidelines for ensuring the effective management of change while reducing risk.	Defined
6.	CLIENTS05-EKS	**Encryption and Key Management Standard**	Standard	This standard establishes requirements for the use of encryption and key management technologies as a baseline for all "CLIENT" operations.	Partially Defined in CLIENTP07-ENP

7.	CLIENTS06-OSS	**Open-Source Software Standard**	Standard	This standard is to provide the minimum information security requirements for using Open-Source Software (OSS) within "CLIENT" development environment.	Not Formally Defined
8.	CLIENTS07-VLS	**Vulnerability Scan Standard**	Standard	This standard provides information security requirements for all applications that may host "CLIENT" data or related customer information, which are required by GRC framework, policy or mandate, to be subject of a vulnerability scan.	Partially Defined in CLIENTP17-VLP
9.	CLIENTS08-DAS	**Data Center Computer Room Security Standard**	Standard	This standard provides guidance on the physical security for rooms or facilities that will house "CLIENT" data.	This standard *may be* partially defined in CLIENTP16-SVP & CLIENTP05-DCP
10.	CLIENTS09-LMS	**Logging and Monitoring Standard**	Standard	This standard provides guidance on the monitoring of the Company's information systems and resources to prevent security controls from being bypassed and identify potential security incidents.	This standard *may be* partially defined in CLIENTP09-MCP
11.	CLIENTS10-IRS	**Incident Response Standard**	Standard	This standard is to establish the requirements for timely reporting, documenting, and investigation of information security incidents within the "CLIENT" computing environment.	Undocumented
12.	CLIENTS11-PTS	**Patching Standard**	Standard	This standard establishes patching requirements for all assets with access to "CLIENT" data, customer data or designated pii.	Partially Defined in CLIENTP14-PMP
13.	CLIENTS12-INS	**Third Party Service Provider Information Sharing Standard**	Standard	This standard establishes requirements for engaging third-party service providers that access, process, store, communicate, or manage "CLIENT" systems, information, or information processing facilities.	Undocumented
14.	CLIENTS13-SVS	**Server Hardening Standard**	Standard	This standard describe the requirements for installing a new server in a secure fashion and maintaining the integrity of the server and application software.	Partially defined in CLIENTP16-SVP
15.	CLIENTR14-DGR	**Digital Application Certification Procedure**	Procedure	This procedure provides definition to and requirements of Digital Application Certification.	Undocumented
16.	CLIENTR15-VLR	**Vulnerability Remediation Enforcement Procedure**	Procedure	This procedure defines the framework for escalation, specifically in instances where there is noncompliance with remediation activities associated with application or infrastructure vulnerabilities.	Undocumented
17.	CLIENTG01-RAG	**RA/RA Guideline**	Guideline	This guideline is proposed for "CLIENT" to roll in its current "IT Risk Assessment Policy."	Undocumented

18.	CLIENTG02-IRG	**Corporate Incident Response Guideline**	Guideline	This guideline establishes the requirements for timely reporting, documenting, and investigation of any information security incidents.	Undocumented
19.	CLIENTP02-AUP	**Acceptable Use Policy**	Policy	Acceptable use of computer equipment at Southeastern Freight Lines.	Defined
20.	CLIENTS16-ACS	**Access Control Standard**	Standard	This standard defines requirements to control access to information and systems on the basis of business, legislative, regulatory, contractual, or information security policies.	Undocumented
21.	CLIENTS19-ATS	**Security Awareness Training Standard**	Standard	This standard defines the requirements for a company-wide Security Awareness Program and ensures the understanding of the Acceptable Use Policy as defined within this ISMS.	Not Formally Defined (although "CLIENT" might be implementing a partial process)
22.	CLIENTS21-PWS	**Global Password Standard**	Standard	This standard provides password requirements for use with all "CLIENT" systems.	Partially documented in CLIENTP13-PWP
23.	CLIENTS22-MBS	**Mobile Device Standard**	Standard	This standard provides requirements for the use of mobile devices, such as smart phones and tablets (including those devices used in all "CLIENT" vehicles).	Currently documented as a Policy. Suggest modifying the current policy (CLIENTP19-MDP) into a Standard and revise accordingly.
24.	CLIENTS23-AVS	**Audio-Video Recording and Photography Standard**	Standard	This standard outlines restrictions for audio/video recording and photographic or image capturing of "CLIENT" data or intellectual property.	Undocumented
25.	CLIENTS24-VUS	**Visitor Acceptable Use Standard**	Standard	This standard outlines CLIENT's visitor acceptable use to safeguard the confidentiality, integrity, and availability of CLIENT-controlled information, information systems, and information processing facilities by specifying acceptable usage of the "CLIENT" guest network for all visitors at any company facilities.	Undocumented
26.	CLIENTS25-NWS	**Social Networking Standard**	Standard	This standard outlines Southeast Freight Lines' expectations for social networking.	Undocumented
27.	CLIENTP03-GVP	**Information Governance Policy**	Policy	This policy addresses the parameters that govern information as a coordinated interdisciplinary approach to optimizing Information value while satisfying legal and compliance requirements and managing Information risks.	Undocumented
28.	CLIENTS26-DAS	**Data Integrity Standard**	Standard	This standard outlines requirements regarding the efficient and effective management of information to ensure data	Not Formally Defined (although "CLIENT" might be implementing a partial

				quality and consistent integrity within key data platforms.	process as part of its “Data Classification Policy”)
29.	CLIENTP04-CDP	**Clean Desk Policy**	Policy	Establish the minimum requirements for maintaining a “clean desk”	Defined
30.	CLIENTP05-DCP	**Data Classification Policy**	Policy	Identify the different types of data, to provide guidelines and examples for each type of data, and to establish the default classification for data. As stated, this policy “might” reference (partially) a Data Center Computer Room Security Standard. (Refer to Line #9 above).	Needs Updating (CLIENTS08-DAS)
31.	CLIENTP06-DBP	**Database Credentials Policy**	Policy	Defines the requirements for securely storing & retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access any “CLIENT” database.	Generic Template / Needs Updating
32.	CLIENTR14-DGR	**Data Governance Procedure**	Procedure	Provides procedural directives for CAB regarding Change Management implementation & oversight	Should be revised
33.	CLIENTP07-ENP	**Encryption Policy**	Policy	Establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption. (Should reference Line #6 above).	Should be revised / Convert to a Encryption and Key Management Standard (CLIENTS05-EKS)
34.	CLIENTP08-ITP	**IT Telecommuting Policy**	Policy	Defines the rules for when employees work at home, on the road or in a satellite location for all or part of their workweek.	Should be revised / Convert to a standard (or combine with Mobile Device Standard)
35.	CLIENTP09-MCP	**Malicious Code Policy**	Policy	Defines a standard for how IDS / SIEM / SOAR capabilities identify and restrict potentially malicious code. (Should reference Line #10 above).	Should be revised / Convert to a Standard (CLIENTS09-LMS)
36.	CLIENTP10-RMP	**Removable Media Policy**	Policy	Defines process to scan all removable media when connected to the local network and from any Southeastern issued devices regardless of local network connectivity or external connectivity.	Should be revised / Convert to a Procedure
37.	CLIENTP11-RAP	**Risk Assessment Policy**	Policy	Currently stated as a policy to validate CIA for Change Management procedures. (Should reference Line #17 above).	Should be revised / Convert to a Procedure and roll into a RA-RA (CLIENTG01-RAG)
38.	CLIENTP12-ACP	**Multi-factor Authentication Policy**	Policy	Currently stated as a definition of requirements for accessing “CLIENT” computer systems containing sensitive data from both on and off campus. (Should reference Line #21 above).	Should be revised / Convert to into Access Control Standard (CLIENTS16-ACS)

39.	CLIENTP13-PWP	**Password Management Policy**	Policy	Describes the "CLIENT" requirements for acceptable password selection and maintenance. (Should reference Line #26 above).	Should be revised / Convert to into Global Password Standard (CLIENTS21-PWS)
40.	CLIENTP14-PMP	**Patch Management Policy**	Policy	Currently provides the basis for maintaining compliance to application and software updates through regular patching. (Should reference Line #12 above).	Should be revised / Convert to into Patching Standard (CLIENTS11-PTS)
41.	CLIENTP15-RMP	**Remote Access Policy**	Policy	Defines standards for connecting to "CLIENT" network from any host.	Defined but suggest revise & modify to a Standard
42.	CLIENTP16-SVP	**Server Security Policy**	Policy	Current Policy describes the requirements for installing a new server in a secure fashion and maintaining the integrity of the server and application software. (Should reference Line #14 above).	Should be revised / Convert to into Server Integrity Standard (CLIENTS13-SVS)
43.	CLIENTP17-VLP	**Vulnerability Policy**	Policy	Current Policy outlines CLIENT's right to scan all network connected devices for vulnerabilities. (Should reference Line #8 above).	Should be revised / Convert to into Vulnerability Scanning Standard (CLIENTS07-VLS)
44.	CLIENTP18-OCP	**OCR Change Management Policy**	Policy	Current Policy outlines the IT Change Management Policy as it pertains to OCR components. (Should reference Line #5 above).	Should be revised / rolled into current Change Management Policy as a sub-category (CLIENTP03-CHP)
45.	CLIENTP19-MDP	**Mobile Device Management Policy**	Policy	Current Policy defines standards, procedures, and restrictions for end users with legitimate business uses connecting mobile devices to "CLIENT" corporate network, digital resources & data. (Should reference Line #27 above).	Should be revised & simplified for easier adoption / Convert to a Mobile Device Standard (CLIENTS22-MBS)
46.	CLIENTP20-BUP	**Back-up & Retention Policy**	Policy	Current Policy is in draft outline form and non-conclusive. (Should reference Line #3 above).	Draft Copy. Should be revised / Convert to an Info Asset Backup and Retention Standard (CLIENTS29-IAS)