Kansas Information Security Office

Information Security Program

**Preliminary DRAFT Plan**

Week of 07/07/2022

*<Agency Name>*

*<Agency ISO Name>*

**Agency Logo

# **Purpose**

The intent of this report is to provide management with a maturity assessment of the (<Agency Name>) (<AGENCY ACRONYM>) information security controls to applicable state or federal regulations and National Institute of Standards and Technology Special Publication 800-53 revision 5, strategic roadmap to mature the information security program, and status of execution towards continuous improvement.

# **Summary**

To develop an effective information security program a security strategy must be defined. Development of a security strategy begins with an assessment of the environment to identify valuable assets, compliance requirements, analysis of controls in place, determination of goals, and recommend actions to achieve those goals.

The results of the initial assessment are anchored by dashboards and reports presenting, the maturity rating of the agency’s information security controls against ITEC policies and NIST SP 800-53 rev 5, strategy to shore up the control environment, execution status (beginning, current, and trend) and its long-term posture on strategy to drive continuous improvement.

# **Security Organization**

Below is an organization chart displaying the composition of (<AGENCY ACRONYM>) Virtual Information Security department. The diagram outlines the roles prescribed by ITEC policies and common security processes. <See ITEC 8010P and 8010A for Roles.>

Create your agency functional security org chart and place it here.



<Agency Name > Functional Security Org Chart

# **DATA Governance & Risk Compliance**

ITEC 7230A 6.3 and 6.4 states entities must ensure that Information Asset Trustees are appointed for Intellectual property or data compilations that contain or may be projected to contain Source Records on thirty (30) or more individuals of Restricted-Use Information.

Depending on the volume and sensitivity levels of the data being managed, some agencies may require more roles than others. At a minimum, agencies must have those roles marked with an asterisk with named and approved individuals.

|  |  |
| --- | --- |
| **Role (Asset Trustees)** | **Responsibility** |
| \*Agency Head | Overall accountability for oversight of state agency data management. |
| \*Information Security Officer | Overall security of agency data and liaison to the Chief Information Security Officer (CISO) of the State of Kansas. Promotes security awareness. |
| Privacy Officer | Provides guidance on privacy laws. |
| \*Data Owner | Security of the data. Accountable to the Agency Head. |
| \*Data Custodian | Protects data from unauthorized access, alteration, destruction, or usage and in a manner consistent with agency policies and policy applicable to the assigned classification level. There are likely to be more than one custodian to represent an agency’s full complement of data assets. |
| \*Records Officer | Ensures an agency’s records are scheduled, retained, and managed in accordance with all state and federal records laws. |
| Data User & End User | Reads and complies with agency data security requirements. |
| System Owner | Develops any additional local requirements, guidelines, and procedures needed to protect the data. |
| Account Administrator | Manages user access and permissions to the data. |

*Data Governance Roles and Responsibilities Matrix*

Agencies storing and collecting data will be able to show an inventory listing of this data that at minimum demonstrates the following:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Type** | **Class.** | **Comp.** | **Loc.** | **Backup Loc.** | **Shared With** | **Recovery Objective** | **Risk If Breached** |
| Credit Card Information | RUI | PCI | TODC | TAPE/ Caves | KDOR | 8 hours | HIGH |
| Federal Tax Information (FTI) | RUI | Pub 1075 | Unisys | Unisys | DCF | 8 hours | HIGH |
| Social Security Information | RUI | SSA | ESOB | Unisys | DCF | 8 hours | HIGH |
| Personally Identifiable Information (PII) | RUI | Privacy Laws | ESOB | Unisys | KDOL | 8 hours | HIGH |

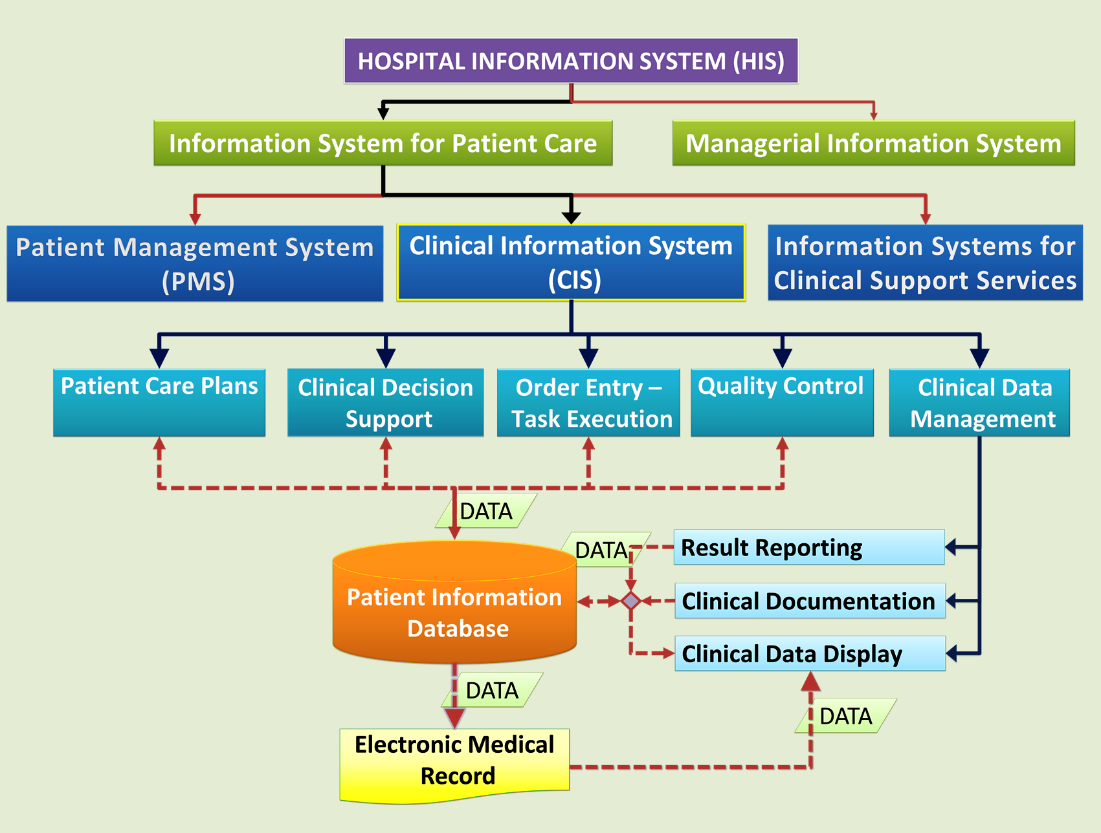
# **Information Systems**

Below you will see a chart of core systems and status of system security plans. This is a very simplified view of security as it relates to business and information systems. This should be followed with a simple diagram showing system linkage of core systems and security systems to an overall secure set of systems and processes as a landscape.

Insert Chart of Core Systems Here

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information System Name** | **Description** | **SSP Status** | **POAM** | **Applicable Compliance** |
| System 1 Example | Provides Human Resources Services to all state agencies | Yes | Yes | PII, HIPAA, PHI |
| System 2 Example | Process the States Financials | Yes | Yes | PII, SOX |
| System 3 Example | Citizen Data and Service Status for KDOT | Yes | Yes |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Insert System Linkage Diagram here**



# **Vulnerability Management**

**Phishing**

# **Maturity Assessment**

The maturity assessment dashboard (above) presents an overview of the <Agency Name> security program scope aligned to the NIST SP 800-53 family of controls, current average maturity rating for agency managed controls and all controls. This is a reference that will be continual updated for regular review and used to track status and drive change.

|  |  |
| --- | --- |
|  |  |

A picture containing chart

Description automatically generated

# **Roadmap**

The security roadmap below has been developed to display the evolution of the agency’s security posture. It highlights major initiatives that advance the agency’s security program to catapult it from one maturity phase to the next. A series of quick hits in PHASE 1 will help quickly shore up some of our current gaps. We will use the results of the Assessment to help us reassess and update our plan and update our roadmap.

The roadmap represents a draft timeline and assumes funding and approvals will occur. The timeline may vary depending on those variables and the degree of difficulty of each step. It should be noted that the team has already taken some steps to make these changes and improvements.

We will conduct on-going regular reviews and self-assessments to drive continuous improvement, help us aligned objectives and budgets and continue to strengthen out posture as the attack surface continues to evolve and change.



**Draft Roadmap**

**Security Posture**

The OITS team has been engaged to manage the agency’s security tools and scanning services. This will include firewall and intrusion protection management, LAN segmenting and assistance in the related reports associated with these services.

These tools and strategies from the OITS team will be rolled out throughout the next several months.

**Security Architecture**

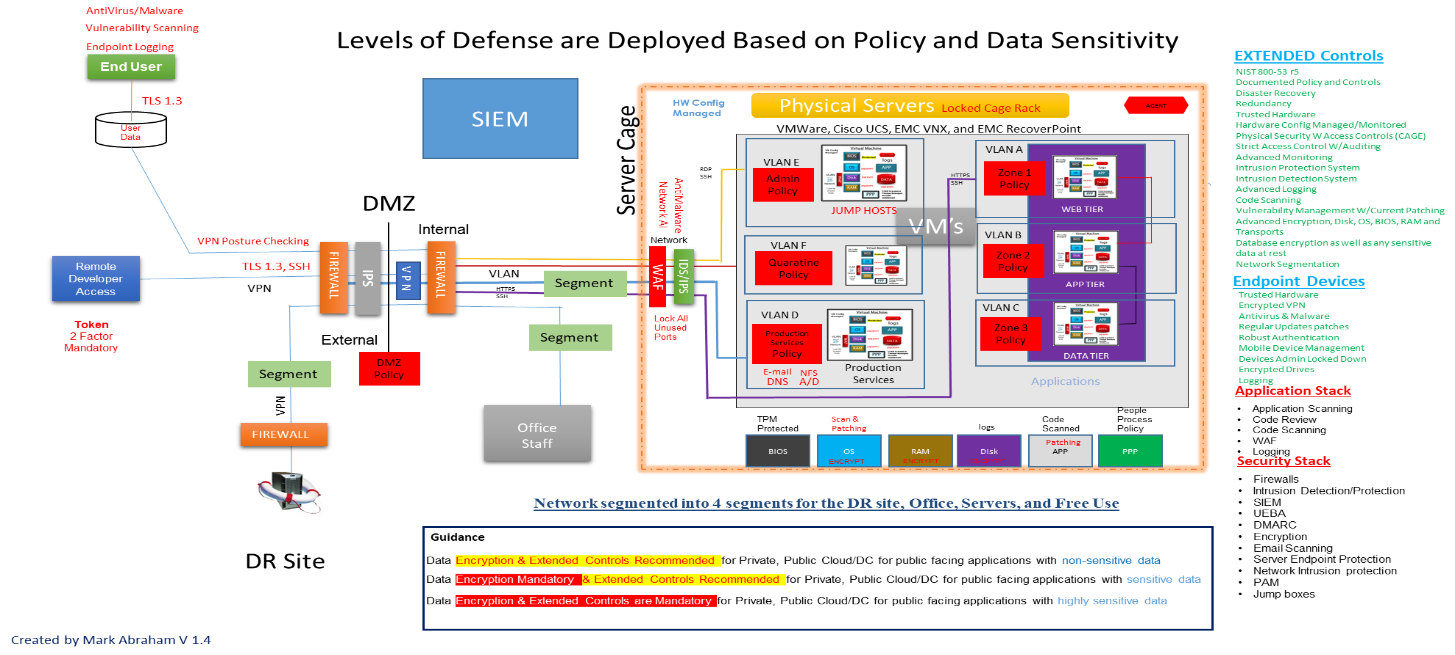
<Agency Names> goal is to adopt and implement security best practice whenever feasible. Exceptions are reviewed and recorded as a part of the agency risk management process.

**Please provide a conceptual diagram like the example below. This can even be borrowed from the reference deck.**

**A picture containing graphical user interface

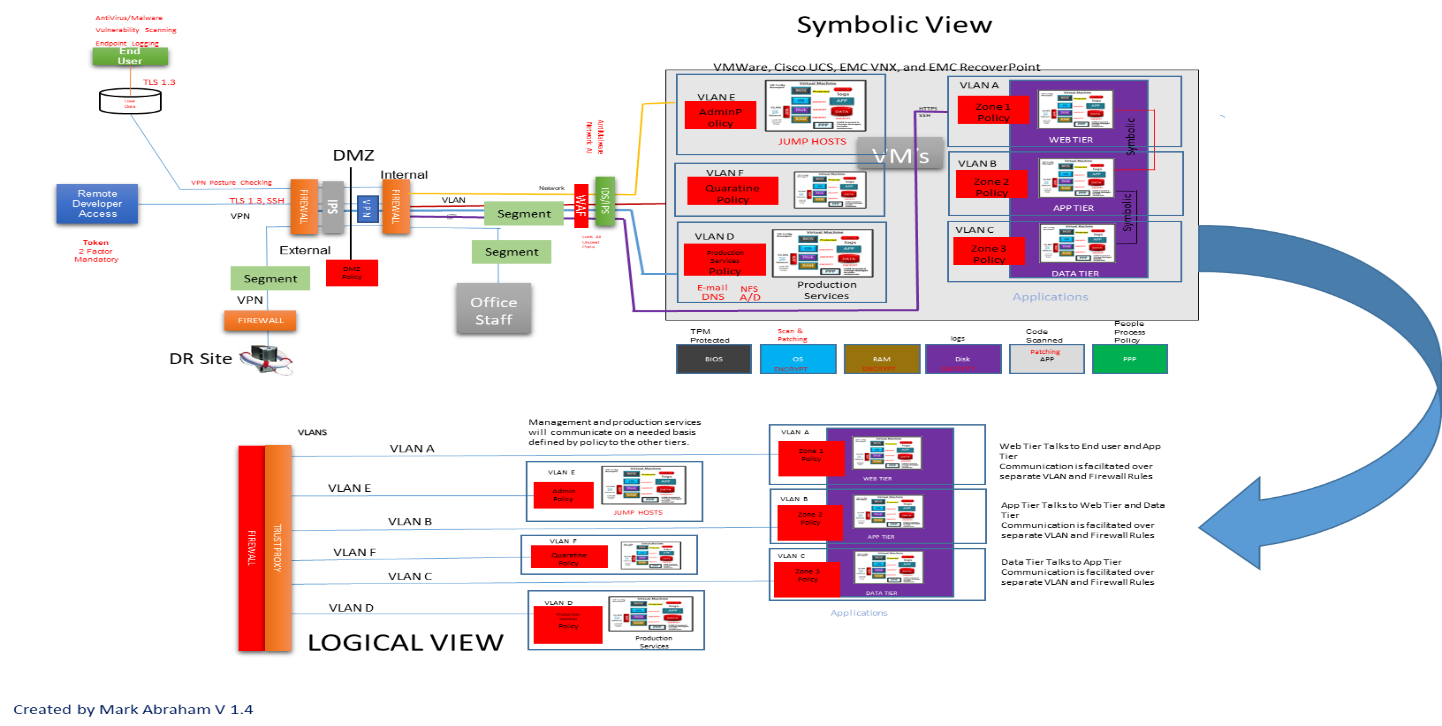
Description automatically generated**

**DRAFT- will be updated with <Agency> Posture**

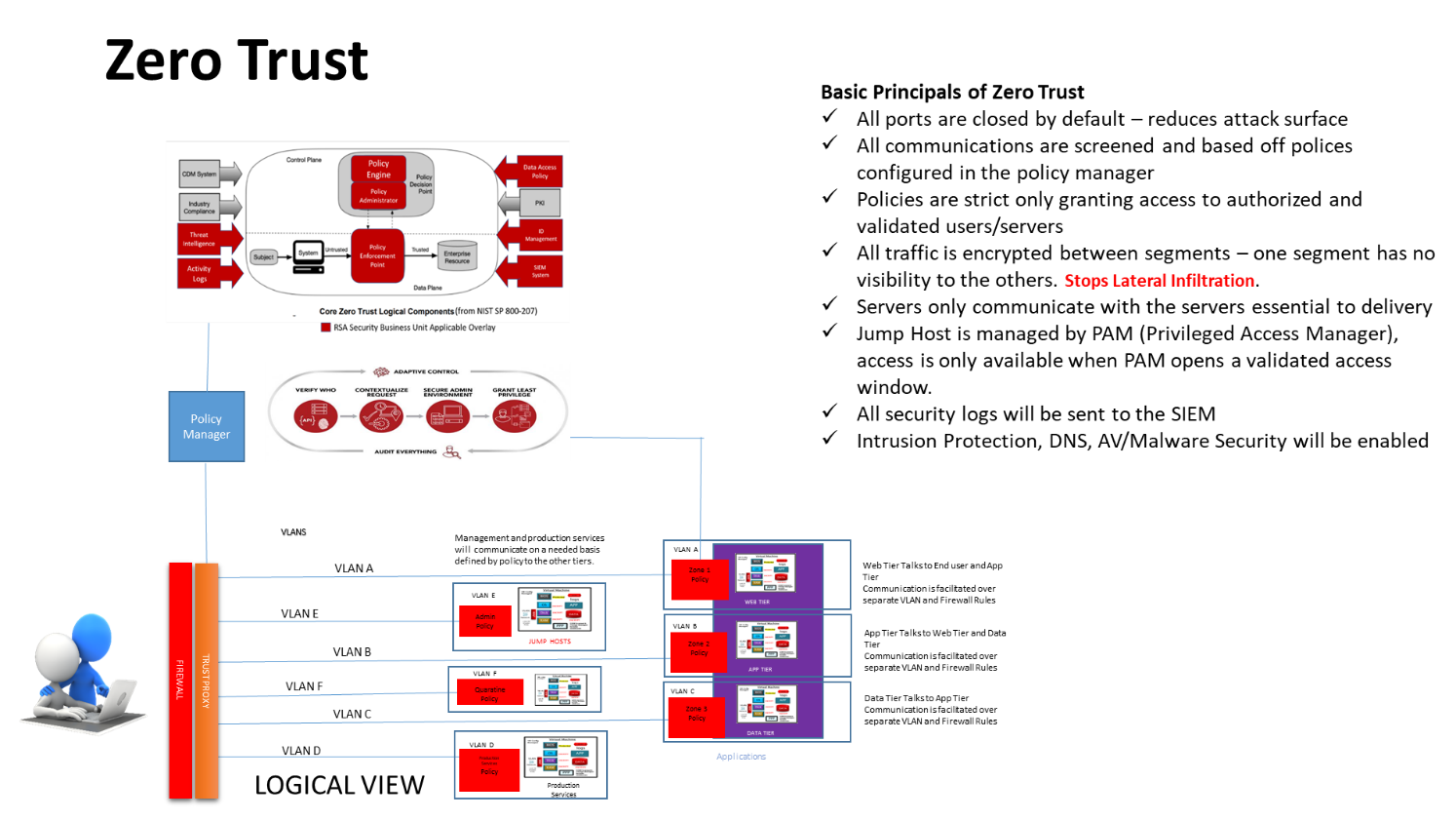
****

**DRAFT – Update with Agency Posture**

The OITS team will assist in updating the security posture as it relates to the areas in the above reference. A walkthrough of the detailed NIST System Integrity Controls is also facilitated.

****

<Agency Name> references the Zero trust model for Cloud Implementations.



<Agency Names> leverage the following services provided by the KISO.

| **Service** | **Description** |  | **Sub Services** |
| --- | --- | --- | --- |
| **Agency Vulnerability Scanning** | These services help agencies identify vulnerabilities on their computing resources such as PC's, Servers and other devices as well as web-based applications. Services available are; Website site Vulnerability Scanning, Endpoint Vulnerability Scanning, Server Vulnerability Scanning |  | * **Nessus Vulnerability Reporting**  - Desktops  - Servers - Nessus Compliance Scanning   **Acunetix Application Scans** |
| **Firewall & VPN Management Services** | These services enable an agency to receive managed firewall services. These include for the agency owned firewalls; managing all the patches, version upgrades, log ingestion, intrusion detection/protection modules installed and installed firewall-based VPN services. This service currently entails a charge back fee based on the number of firewalls and complexity of the agency’s environment. This service enables an agency to host their firewall on our shared firewall server. Virtualized firewalls come with Intrusion protection, Antivirus/Malware Protection, Threat Intelligence, DNS Filtering, Logging, URL lso filtering and VPN Services. Virtual Firewalls are configured to the agency compliance requirements. The firewalls are all managed for the agency. |  | Agency FW Management  Threat Protection FW DNS Protection  FW URL FILTERING  VPN Virtualized Firewall |
| **Azure Cloud Security Services** | KISO has a GOV Cloud Security Tenant to support GOV Cloud hosting with SIEM and Compliance monitoring along with Azure FW. |  | Cloud Security Support  Azure Security Center  Azure SIEM  Azure FW Compliance Reporting |
| **Continuous Monitoring** | These services enable the agency to leverage the states enterprise Security Information Event Management (SIEM) system. Services include security logging, compliance monitoring, threat intelligence, alerting, SIEM Dashboard Reporting, Tier 1 Incident Investigation & Response and endpoint advanced endpoint protection agent (CrowdStrike Falcon). |  | SIEM Continuous Monitoring  SIEM (Enhanced) Continuous Monitoring  Event Reports  Reporting (Future service being defined)  User Behavioral Analytics  Log Storage (Basic)  Log Storage (Enhanced)  Incident Response (available Logs & Forensics - ) AV/Malware Endpoint  Advanced Endpoint Detection& Response  Network Detection and Response  Compliance Reporting Cyber Hygiene Scoring & Reporting |
| **Project Security Consulting Support** | This service is charged back to the agency $100 per hour and provides project support, security architecture consulting, special project security device configuration support, Azure Security Tenant Support & troubleshooting. These services also allow agencies to use the shared RSA MFA Token Server and the ability to request domain webserver certificates through our shared Entrust Tenant. |  | ISO Support  COOP Planning  Agency Assessments  Security Awareness Training Project Consulting Security Architecture RSA Token Support  Entrust Certificates Vendor Remote Access Authentication Consulting |

The Security Program is managed by the ISO for the agency and will be reviewed quarterly with leadership.

**DOCUMENT CONTROL**

| **Version #** | **Implemented By** | **Revision Date** | **Reason** |
| --- | --- | --- | --- |
| 1.0 | Mark Abraham – Deputy ISO | 7/31/2018 | Initial Template - Remove |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |