**Project**: Information Security Management Systems Guidelines using National Institute of Standards and Technology (NIST) and Centre for Internet Security (CIS).

**Organisation**: Oil and Gas Free Zones Authority | <https://ogfza.gov.ng/>

**Project Objective**:

* This guideline describes a set of best IT practices intended to ensure effective implementation of industry-standard requirement for information security management programs.
* The purpose of this document is to provide an understanding of the specific, standards-based security controls as required by NIST and CIS to guarantee best cybersecurity program.

Strategic objectives accompanying this guideline are:

* Implementing a robust cybersecurity awareness program and ensuring that end-users are informed of the criticality of protecting sensitive information and the risk of mishandling information.
* Implementing adequate security controls to meet the existing information protection needs and demand of the future based on changing threats landscape and emerging technologies.
* Laying a foundation for the development of risk assessment methods internally and procedures for determining the effectiveness of the implemented security controls.

**Executive Summary**

Businesses are taking advantage of the advances in internet technology. Cloud computing and Internet of Things (IoT) are rapidly changing the way businesses are conducted. The COVID19 pandemic has thrown up new challenges, causing many organizations to migrate their business workload to the cloud to continue to serve their customers and stay in the business.

While the cloud promises agility and business efficiency, it has also presented another challenge to organizations adopting the technology. Migration to the cloud means that part or the whole of organizations traditional on-premises computing infrastructure and digital assets are moved to the cloud.

With the movement of critical digital assets to the digital, organizations have expanded their attack surface, given the increasing cases of reported cyber-attack, the threats landscape becomes larger by the day.

It has therefore become imperative that Oil and Gas Free Zones Authority (OGFZA) prepares in event of any security threat.

It is on the strength of the above that the development of a Technology Strategy Guideline has become a necessity.

The purpose of this guideline is to develop an information security management system taking into consideration the requirements of the National Institute of Standards and Technology (NIST) and Centre for Internet Security (CIS).

NIST has developed a Cybersecurity Framework to guide organizations in implementing their IT security guidelines. CIS has developed Top 20 Critical Security Control Solutions that should be implemented by organizations to provide effective security controls against real-world cyber threats.

**Background:**

The increasing number of cyberattacks on large and small businesses is a walk-up call that we should do something early to prepare our organization for such contingency. They cannot be any right time other than now.

As the Chief Information Security Officer of this organization, it is my responsibility to ensure that we have implemented holistic preventive security controls in our organization to stay safe from threats of any kind.

I, therefore, feel an obligation to develop cybersecurity implementation guideline for Oil and Gas Free Zones Authority.

**Purpose of the Guideline:**

This guideline describes a set of best IT practices intended to ensure effective implementation of industry-standard requirement for information security management programs.

The purpose of this document is to provide an understanding of the specific, standards-based security controls as required by NIST and CIS to guarantee best cybersecurity program.

Strategic objectives accompanying this guideline are:

* Implementing a robust cybersecurity awareness program, and ensuring that end-users are informed of the criticality of protecting sensitive information and the risk of mishandling information.
* Implementing adequate security controls to meet the existing information protection needs and demand of the future based on changing threats landscape and emerging technologies.
* Laying a foundation for the development of risk assessment methods internally and procedures for determining the effectiveness of the implemented security controls.

**Organization of the guidelines:**

**Definition of cybersecurity:**

NIST defines cybersecurity as the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

**NIST Cybersecurity**

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks (Wikipedia).

**The CIS Critical Security Controls for Effective Cyber Defense:**

The Center for Internet Security Critical Security Controls for Effective Cyber Defense is a publication of best practice guidelines for computer security. The project was initiated early in 2008 in response to extreme data losses experienced by organizations in the US defense industrial base (Wikipedia).

**Organization of NIST Cybersecurity Framework and CIS Security Controls:**

NIST publishes guidance documents under its Special Publications (SP) 800 series. The 800 series reports on the Information Technology Laboratory’s (ITL) research and guidelines. NIST SP 800-53 deals with the security controls or safeguards for federal information systems and organizations (Lord, 2018). The framework provides core controls and processes in critical areas for effective implementation of cybersecurity. It defines the five concurrent functions **Identify, Protect, Detect, Respond, Recover**. Several of these functions relate to processes and policies. The Protect function, in particular, relates to concrete protections that need to be implemented for systems and data (SSH Academy, n.d.).

NIST security controls are broken into 3 classes depending on impact – low, moderate, and high – and split into 18 different families:

Graphical user interface

Description automatically generated

Image Credit: https://www.securityinfowatch.com/

The Center for Internet Security Critical Security Controls for Effective Cyber Defense is a publication of best practice guidelines for computer security. The guidelines consist of 20 key actions, called critical security controls (CSC), that organizations should implement to block or mitigate known attacks:

**Graphical user interface

Description automatically generated**

Image Credit: https://skylinenet.net/initiatives/cyber-security-plan

**Obstacles to achieving goals:**

There may be two fundamental reasons for not achieving a cybersecurity strategic plan. Inadequate budgetary provision for the cybersecurity program and the lack of knowledgeable personnel in the organisation. To address these gaps, the Board of Directors needs to ensure the budget for planned cybersecurity programme receives approval from the appropriate authority. On the issue of skilled manpower, the organization can leverage a managed services provider who has the appropriate technology, level of skill, experience and understanding of IT systems.

**Long-term Goals:**

To develop an agile, effective, and cost-efficient approach to cybersecurity aligned with the current threats and adaptable to OGFZA's business objective.

**Short-term Goals:**

**Year 1**: Protect OGFZA's information and information systems to ensure that the confidentiality, Integrity, and Availability of all information is commensurate with the mission needs, information value and associated threats.

**Year 2**: Enable advanced cybersecurity capabilities at all functional levels of the organization.

**Year 3**: Develop a cybersecurity knowledgeable workforce.

**Benchmarks of Success:**

By benchmarking the organization’s cybersecurity performance, it is possible to identify weaknesses, better prioritize remediation, clearly track performance, and help improve communication between IT and senior leadership.

Cybersecurity effectiveness can be calculated by how much time lapses between the detection of a threat and when appropriate action is taken. An organization needs to find an objective method of calculating recovery time (Solis Security, n.d.).

**Framework Implementation Overview**

**Cybersecurity Strategic Guideline**

In developing this guideline, we followed the industry standard. The following are the steps used in preparing this guideline:

**Define the organization’s cybersecurity objective** – This entails defining the goal of the organization’s cybersecurity program. Set the acceptable level of risk, define cybersecurity budget, and get stakeholders and employee buy-in on the cybersecurity governance.

**Create the organization’s security profile** – This is done to tailor the framework to the specific security needs of the organization. This is executed using the framework implementation tiers - Risk Management Process, Integrated Risk Management Program, and External Participation.

**Assess the organization’s current security situation** – An independent risk assessment is carried out at this stage to establish the current security situation in the organization.

**Analysis of Gaps and Identification of Actions Necessary** - Given a deep knowledge of cybersecurity risks and the potential business impacts for your organization, gap analysis is conducted by comparing the targeted security objective with the existing security objective. The purpose is to develop an implementation action plan to close the gaps. This could be in the form of budgetary provisions, staffing, meeting project requirements and getting stakeholders approval for these actions.

**Implementation of the Action Plan** – With a clear understanding of the cybersecurity situation, a set of organizationally aligned target objectives, comprehensive gap analysis and a set of remediation actions, implementing the NIST CSF is ready. This involves developing processes and training materials for implementation. The framework is at this point adapted to fit the organization based on the organization’s peculiarity.

**Risk Management**

People, process, and technology are integral parts of the organization that should be aligned to achieve cybersecurity objectives. Proper security controls should be put in place to ensure protection against data breaches. Security risk analysis is an area of enterprise risk management system that should be performed to determine the risk level and method of handling the risk.

Risk management will incorporate multiple systems to deal with information security risks that affect operations. The process will include creating a framework to recognize activities, analyze the risk, create a solution to combat the risk, and to keep up with dealing with risk over an extended period. The system will be such that can address the risk to the organization.

**Proposed Budget**

For an effective cybersecurity implementation program, budgetary provision must be made to cover the funding required to execute it. As with a component of business, there are a lot of factors that determine how to build a cybersecurity budget. Key considerations are:

* Industry and size of the organization.
* Compliance and regulation requirements as it affect the business.
* The sensitive nature of the data the organization holds.
* Request from company stakeholders or customers.

Cybersecurity budget is usually built into IT spending and depends on the company size and IT infrastructure available.

At the very basic, if an enterprise-wide endpoint security software (Kaspersky Cloud) is used, licensing for OGFZA’s 300 users would amount to N1,200,000 million (at N41,000 per 10 users)

Physical Firewall – N500,000

Microsoft Defender 365 (ATP) for hosted email for 300 users at N12,000 would amount to N3,600,000

Security for Sever Operating System = N100,000

Training and Cybersecurity awareness program – N2,000,000

Backup solution – N500,000

Compliance and regulatory spending N5,000,000

**Estimated Annual Budget for an Effective Cybersecurity program for OGFZA:**

Compliance and regulatory spending – N5,000,000

Enterprise-wide Endpoint Security Solution - N1,200,000

Microsoft Defender 365 – N3,600,00

Hardware Firewall – N500,000

Software Firewall (annual licensing) – N200,000

Backup Solution – N500,000

Training and Cybersecurity awareness program – N2,000,000

Total Annual Proposed Budget = (N5,000,000 + N1,200,000 + N3,600,000 + N500,00 + N200,00 + N500,000 + N2,000,000) = **N13,000,000 = $35,000 for a year**.

A comprehensive cybersecurity program does not have to cost a lot of money, but it does require prioritization and commitment from leadership, IT and employees (Rinaldi, 2020).

**Human Resources required to successfully implement this guideline.**

Human Resources have become integral to organizational cyber risk management in recent years due to a convergence of factors: an increasingly active regulatory environment, the pervasive use of technology and devices in employees’ work, and recognition of the importance of a strong organizational cybersecurity culture (Marsh, n.d.).

For effective implementation of this guideline, the following human resources are required:

* The stakeholders
* Management and leadership
* Employees (non-technical users)
* Employees in the IT department
* External (independent assessor)

**Steps to Implementation of the CIS Critical Controls / Framework**

NIST recommends that organizations implement this process in order to best establish or update cybersecurity programs. Cybersecurity programs, or proposed programs, are compared to the five high-level functions of NIST CSF (Belding, 2019).

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyse, and Prioritize Gaps
7. Implement Action Plan

**STEP 1: Prioritize and Scope** – This involves inventorizing important organizational assets and prioritizing them in order of the protection level they require, starting with low-priority one. The organization should at this level make a strategic cybersecurity implementation decision and determine the scope of all systems with the organization

**STEP 2: Orient** – At this level, the organization should identify related systems and assets, regulatory requirements, and the risk approach to be used in the program. Vulnerabilities and threats to the systems and assets should be identified.

**STEP 3: Create a Current Organizational Profile** – Profiling, in this case, means identifying the existing security controls and comparing them against the NIST CSF in order to determine the ones that meet the baseline requirement, and the ones that should be implemented afresh.

**STEP 4: Conducting a Risk Assessment** – A risk assessment should be conducted to determine the organization’s overall risk management approach. This helps to identify the areas of a possible cybersecurity event and related impact.

**STEP 5: Create a Target Profile** – The organization should at this point create a target profile that focuses on the CSF Categories and Subcategories assessment and describes the desired cybersecurity outcomes. Based upon the organization’s specific needs, extra categories and subcategories of control can be added.

**STEP 6: Determine, Analyse and Prioritize Gaps** – Based on the existing and target profiles, a gap analysis should be performed to determine and prioritize action plans that should be implemented to address the gap found. This is where the use cost, the benefits, risks, and mission-driven considerations to achieve the target profile is established.

**STEP 7: Implement Action Plan** – After identifying all the steps needed to be taken to address the gaps presented above, the organization can then determine which course of action to take and carry out said action to fully address the gaps. Cybersecurity practices can be adjusted to achieve the target profile.

**Monitoring:**

Proactive and continuous cybersecurity monitoring has become a necessity in an organization. It provides a constant, full assessment of the organization's enterprise network so that the IT team can stay ahead of the hackers and prevent breaches. This is only the way the IT team can determine the cyberhealth of the organization**.**

Tools that should be used to provide visibility into gaps within network security include:

* Threat prioritization.
* Visibility into a third-party vendor’s network
* Reports catered to management.
* Streamlined record keeping.
* Risk analytics.

**Conclusion and Recommendations**

The NIST Cybersecurity Framework is used to enable end-to-end risk management across organizations where senior-level communicates mission priorities, resources, and level of risk tolerance to the business level. This can then be used to develop a profile to coordinate operations and implementation activities. The operations level uses this to determine impact, which is provided to the business level management to report out to ensure senior-level management is cognizant of the business impact. Overall, the cybersecurity program is required to be consistently adjusted based on the specific needs of the organization to guarantee a successful security program across all functional level of the organization.

**Appendices:**

|  |  |  |
| --- | --- | --- |
| CIS 20 Security Controls | | |
| **CIS Control** | **Title** | **Description** |
| 1 | **Inventory and Control of Hardware Assets** |  |
|  | *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.* | |
| 2 | **Inventory and Control of Software Assets** |  |
|  | Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. | |
| 3 | **Continuous Vulnerability Management** |  |
|  | *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.* | |
| 4 | **Controlled Use of Administrative Privileges** |  |
|  | *The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.* | |
| 5 | **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** |  |
|  | *Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.* | |
| 6 | **Maintenance, Monitoring and Analysis of Audit Logs** |  |
|  | *Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.* | |
| 7 | **Email and Web Browser Protections** |  |
|  | *Minimize the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems.* | |
| 8 | **Malware Defences** |  |
|  | *Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.* | |
| 9 | **Limitation and Control of Network Ports, Protocols, and Services** |  |
|  | *Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.* | |
| 10 | **Data Recovery Capabilities** |  |
|  | *The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.* | |
| 11 | **Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** |  |
|  | *Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.* | |
| 12 | **Boundary Défense** |  |
|  | *Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.* | |
| 13 | **Data Protection** |  |
|  | *The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.* | |
| 14 | **Controlled Access Based on the Need to Kno**w |  |
|  | *The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.* | |
| 15 | **Wireless Access Control** |  |
|  | *The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.* | |
| 16 | **Account Monitoring and Control** | |
|  | *Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.* | |
| 17 | **Implement a Security Awareness and Training Program** |  |
|  | *For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.* | |
| 18 | **Application Software Security** | |
|  | *Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.* | |
| 19 | **Incident Response and Management** |  |
|  | *Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.* | |
| 20 | **Penetration Tests and Red Team Exercises** |  |
|  | *Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.* | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Semi-Complete Technology Implementation Plan Matrix | | | | | | |
| **Task No.** | **Task** | **Method of implementation** | **Responsible  party** | **Stakeholder** | **Budget/Source** | **Time frame  for completion** |
| Creating information security policy for compliance with the requirement of National Information Technology Development Agency Data Privacy/Protection Guideline 2020 | | | | | | |
| 1.1 | Activate organizational  processes to comply with NITDA Nigeria Data Protection  Regulation Guidelines 2020 | Appointment of an Independent Data Protection  Compliance Organization (DPCO) and Data Protection Officer  (DPO) to carry our independent assessment of OGFZA's  NDPR compliance activities | ICT Department | Management | N2,500,000 | 1 March 2021 |
| Conduct an assessment of the existing organisational environment and determine the existing security controls and what has not been implemented as required by NITDA | | | | | | |
| 1.2 | DPCO to conduct an assessment of the existing  environment | DPCO to conduct a comprehensive assessment of the current  security controls and determine where we are, and where  ought to be | DPCO | DPO | N1,000,000 | 1 April 2021 |
| 1.3 | Determine organizational assets and prioritize | Take inventory of all organizational assets and assign  priority according to the protection required | ICT Department | Management | N500,000 | 1 May 2021 |
| Develop Information Security Policies to guide stakeholders and employees within the organization | | | | | | |
| 1.4 | Develop IT policies | Develop Computer use policies, email use policy, Acceptable  use policy, etc | ICT Department | Management | N1,200,000 | 1 June 2021 |
| Determination of Risk Management and Communications System between Stakeholders | | | | | | |
| 1.5 | Implement a system for reporting and responding to security incidents | Implement a cloud-based reporting system lodging incident  report | ICT Department | Management | N2,000.000 | 1 July 2021 |
| Implementation of Security Controls as required by NIST and CIS | | | | | | |
|  |  |  |  |  |  |  |
| 1.6 | Implement security controls | Implement all the necessary controls according to organization specific needs. This involved procuring all needed security solutions | ICT Department | Management | N15,000,000 | 1 August 2021 |
| Implementation of Awareness System and Cybersecurity Education for Employees and Stakeholder | | | | | | |
| 1.7 | Create a cybersecurity  awareness | Launch a series of cybersecurity awareness program to educate employees and stakeholders on roles expected of them | ICT Department | Management | N1,000.000 | 8 September 2021 |
| 1.8 | Create a cybersecurity  culture | Stakeholders’ engagement is needed here to create a  cybersecurity | ICT Department | Management | N2,000,000 | 1 October 2021 |

**References:**

Belding, G. (2019, December 23). NIST CSF: The Seven-Step Cybersecurity Framework Process. Infosecurity Institute. <https://resources.infosecinstitute.com/topic/nist-csf-the-seven-step-cybersecurity-framework-process/>

Kim, L. (2019, August 30). Cybersecurity Frameworks Explained. Healthcare Information and Management Systems Society. https://www.himss.org/resources/cybersecurity-frameworks-explained#

Lord, N. (2018, September 11). What is NIST SP 800-53? Definition and Tips for NIST SP 800-53 Compliance. Digital Guardian. <https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance>

Marsh. (n.d.). Human Resources’ Increasing Role in Cyber Risk Management. Retrieved November 23, 2020, from <https://www.marsh.com/us/insights/research/human-resources-role-increase-cyber-risk-management.html>

NIST. (n.d.). cybersecurity. Retrieved November 22, 2020, from <https://csrc.nist.gov/glossary/term/cybersecurity>

Rinaldi, A. (2020, October 15). The Cost of Cybersecurity and How to Budget for it. Business.Com. <https://www.business.com/articles/smb-budget-for-cybersecurity/>

Solis Security. (n.d.). How Do You Measure Your Company’s Cybersecurity Effectiveness? Retrieved November 24, 2020, from <https://www.gosolis.com/technology-news/how-do-you-measure-your-companys-cybersecurity-effectiveness/>

SSH Academy. (n.d.). NIST Cybersecurity Framework. SSH.COM. Retrieved November 22, 2020, from [https://www.ssh.com/compliance/cybersecurity-framework/#](https://www.ssh.com/compliance/cybersecurity-framework/)

Wikipedia. (n.d.). NIST Cybersecurity Framework. Retrieved November 22, 2020 from <https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework>

Wikipedia. (n.d.). The CIS Critical Security Controls for Effective Cyber Defense. November 22, 2020, from <https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense>