An introduction to G-SOS (Green - Secure; Optimize and Strengthen) as a Board Room Strategy to combat cyber security risk

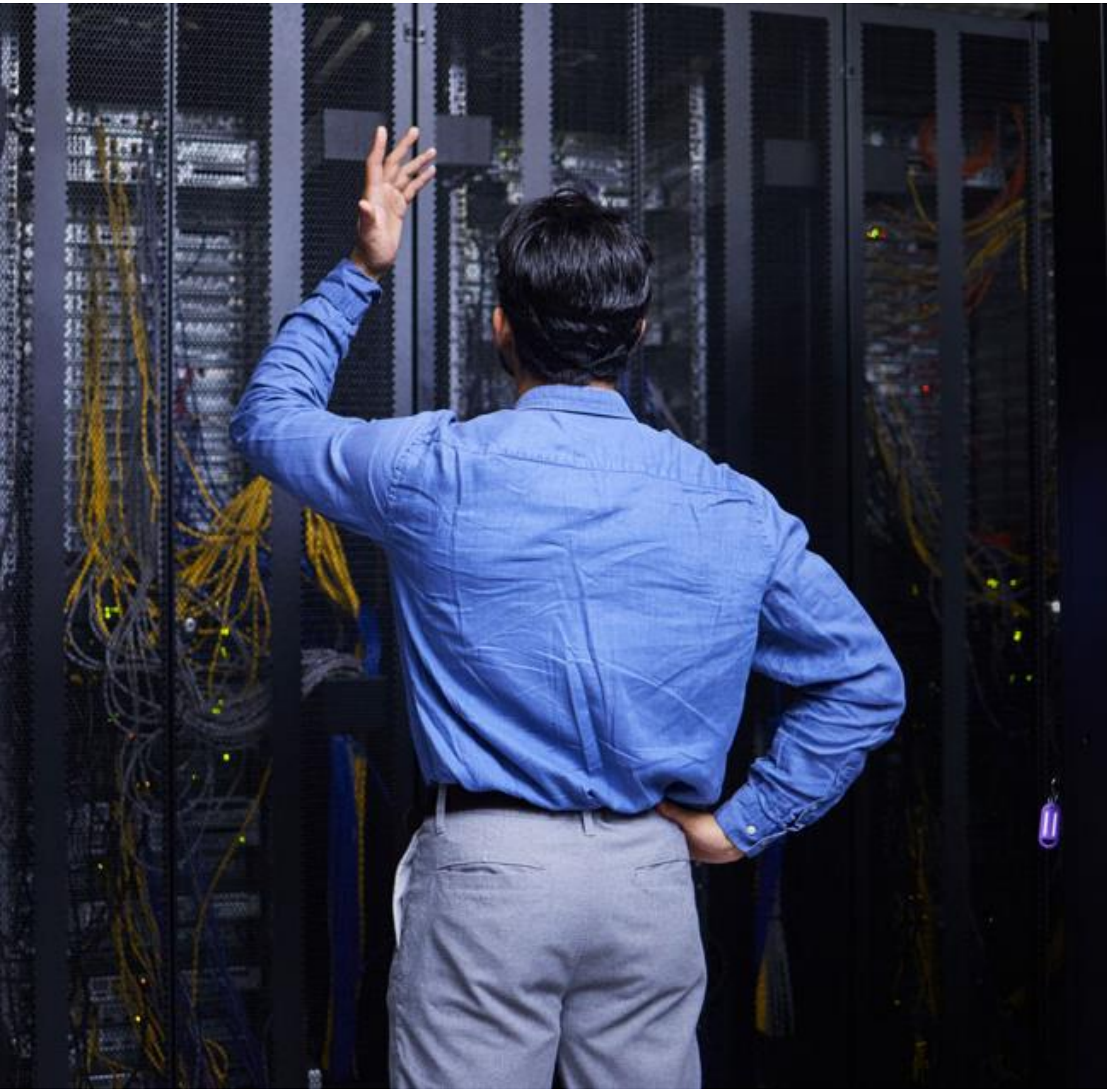


Table of Contents

Contents

Setting the Context

This whitepaper explores an approach where we can bring together an integrated platform consisting of strategy, solutions, and services to effectively identify, treat and measure Cyber Risks across the Board. As any reader is aware, any organization today is bound by multiple compliance and regulatory requirements for security and that in the absence of an integrated approach, it is highly impossible to manage the Cyber Risks in a way that is aligned with the overall strategic direction of the company.

Current Challenges:

Currently the way in which Cyber Risks are managed is ad-hoc and there is no holistic view or approach to this. There is no one-stop solution that manages the Cyber Risks and provide insights and aides the management in the decision-making process. This has a put a lot of strain on the Board / the Top Management who is eventually accountable for Cyber Security Risks. There are multiple compliance requirements, multiple point technologies, various different teams with independent focus, various processes and Risks not being identified at organizational level. What is missing is a coercive approach to bring together various Governance, Risk and Compliance Programs under one umbrella with a definite vision and mission to manage Cyber Risks across the organization.

What shall be the approach then?

What we need in such a scenario is an Integrated platform that brings together the strategies, services, and solutions, it takes to identify and manage Cyber Risks on an ongoing basis. We achieve this by developing an integrated platform that addresses key elements such as defining the overall vision and mission of the organization for cyber security management, developing an Enterprise Risk Management module, Centralised Control Assurance & Monitoring Program and Organization Wide Awareness Programs. This is followed by other key components as in Board Room War Games to test the efficacy of the Programs on an Ongoing basis and implementing SOS Program Dashboards to measure and monitor the progress of the program on a continuous basis. The underlying approach is to enhance the Cyber Security Posture of an Organization in a phased manner from Secure phase to Optimize phase to the Strengthen phase.

G-SOS Strategy

The main objective of a G-SOS strategy is to establish an integrated platform to effectively establish a Governance, Risk and Compliance Framework that addresses Cyber Risks at Organization level and help the Board / Top Management make decisions on an Ongoing Basis.

This product is a strategic tool focusing on governance, strategy, risk and compliance. This board room tool provides a deep insight on the organizational structure, the vision, the mission, the existing context, the future road map, the plans supporting the strategies, the control system designed and implemented, the metrics, the dashboard, the pivotal risk management component, the communication strategy, the awareness building mechanisms, the control mapping to various international best practice standards and guidelines etc.

This is an integrated platform designed to integrate all the Compliance related best practices into everyday business processes which is indeed the need of the hour.

This platform helps to manage your entire IT landscape, infrastructure, control systems, people and creates a stronger security, risk management, assurance and compliances across the organization. This helps to streamline the operation, effective implementation of various best practice control system, governance and monitoring through a dashboard which provides the overall health of your system. It’s very correctly said “What gets monitored and measured, gets improved”.

Organizations can define their own customized control system environment, type of activity, all kinds of laws and compliance requirements based on standards, guidelines, contractual requirements which needs to be implemented internally and enforced across the organization without much pain and efforts.

This tool helps to identify and mitigate all types of risk including service delivery risk/ quality risks, security risks, privacy risks, continuity risks, technology risks, logical risks, people risks, physical and environmental risks and helps monitor company-wide strategies for risk management.

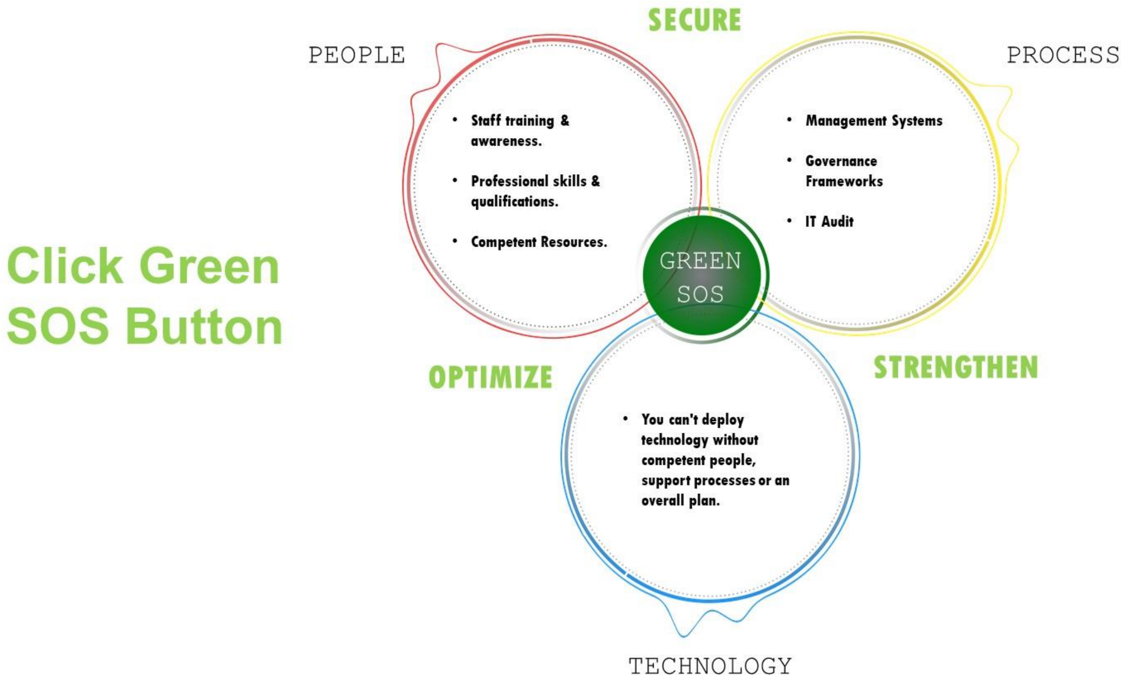

SECURE
PEOPLE
PROCESS
Staff training & awareness.
Professional skills & qualifications.
Competent Resources.
Management Systems
Governance Frameworks
IT Audit
Click Green SOS Button
GREEN SOS
OPTIMIZE
STRENGTHEN
You can't deploy technology without competent people, support processes or an overall plan.
TECHNOLOGY

Figure 1 We are using Secure; Optimize and Strengthen as a Strategy that cuts across People, Process and Technology paradigm.

SOS:

SECURE system components

Design system components

OPERATE AND OPTIMIZE system components effectively

Monitor and measure

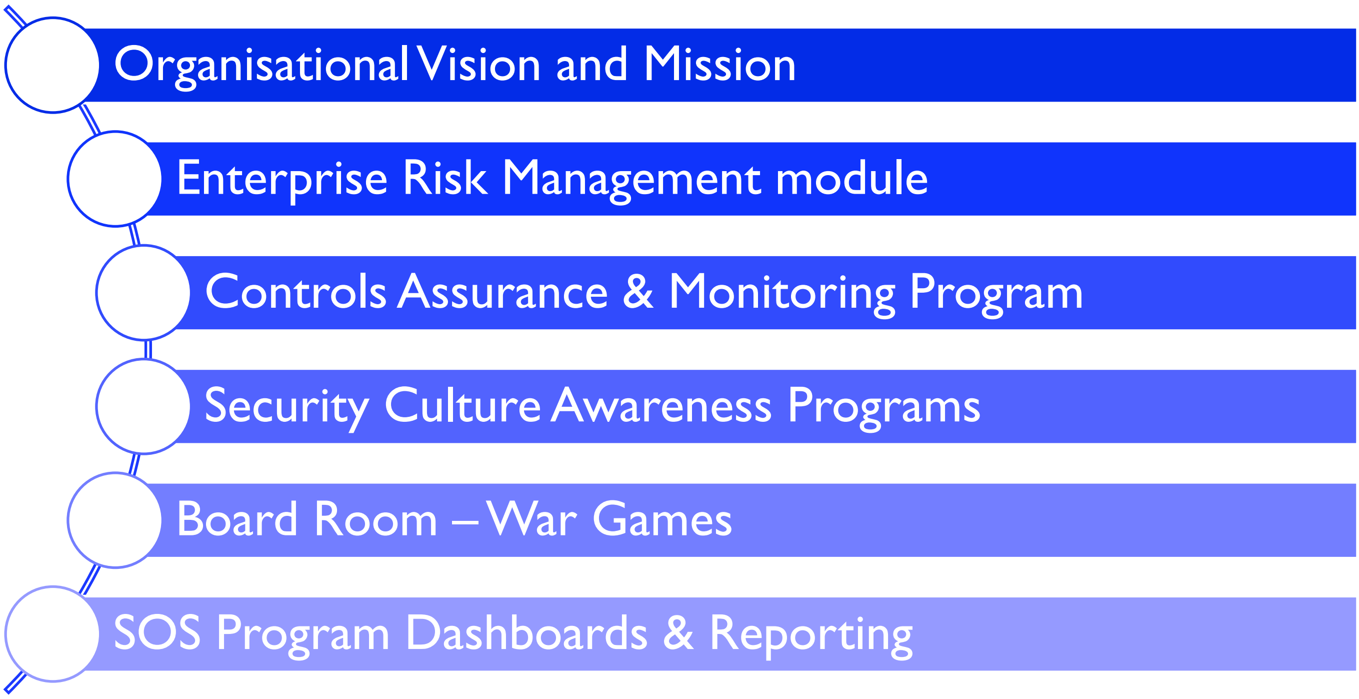
Improve and **STRENGTHEN**

As can be seen, there is a maturity curve that any organization has to pass through to achieve the desired level of maturity when it comes to its overall Cyber Security Posture. The G-SOS Strategy is also greatly tied to the Cyber Security maturity enhancement program that any organization undertake.

The initial phase is to identify and secure the system components that comprise the overall cyber security program. Once that is inventoried, the next logical step is to Design the control environment per the leading compliance practices, frameworks and standards. Post that the Operating Effectiveness of the Controls are tested and Optimized to arrive at the desired maturity level that gives confidence to the Key Stakeholders. This shall need to be Monitored and Measured for the period in consideration. The last and most pivotal step is to Improve and Strengthen the Overall Cyber Security Governance, Risk and Compliance Program to be robust and world-class in alignment with the Strategic Direction of the company.

G-SOS Components

It constitutes the following modules:



Organisational Vision and Mission

Enterprise Risk Management module

Controls Assurance & Monitoring Program

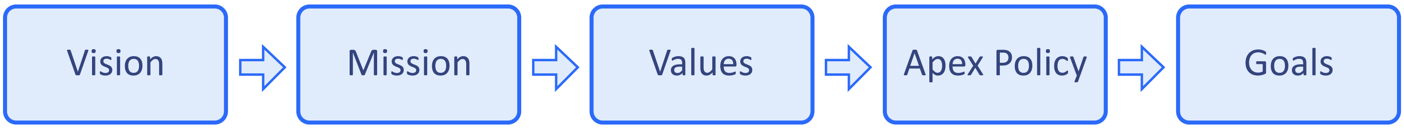
Security Culture Awareness Programs

Board Room – War Games

SOS Program Dashboards & Reporting

1. Organizational Vision and Mission:

This is the initial and the most crucial phase where the organization define the goals for the Organization Wide Cyber Security Posture enhancement program. It starts with the Vision and Mission of the organization and require the contribution of all the key stakeholders to arrive at SMART Goals that is in alignment with the Business Strategy of the Organization.

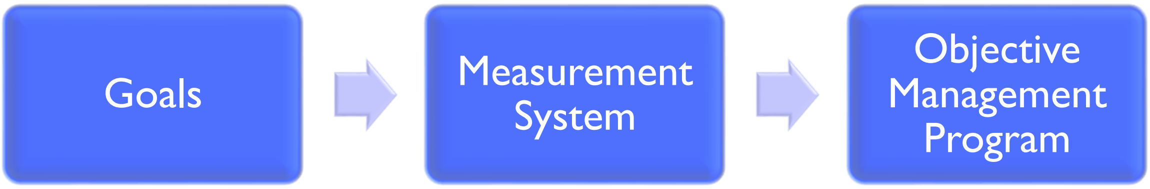


Vision → Mission → Values → Apex Policy → Goals

GOALS

For effective   governance; establishing the goals is very essential at various levels. Establishing SMART goals/objectives and tracking them is essential for effective governance. Plans shall be established to achieve the goals in a defined period.

Smart Goals lead to a Measurement System that eventually result in an Objective Management Program.

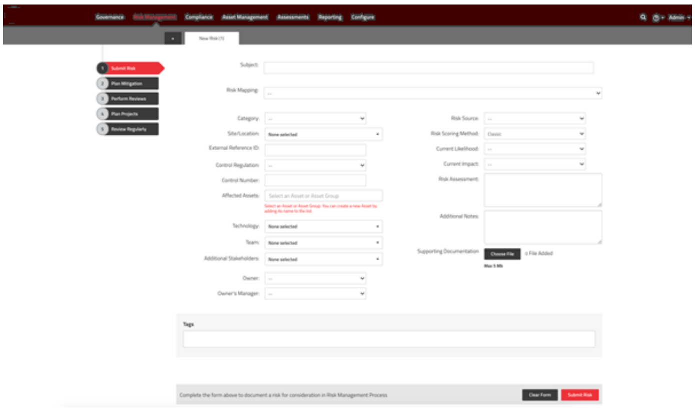


Goals → Measurement System → Objective Management Program

2. Enterprise Risk Management Module:

Enterprise risk management activities are designed to ensure that management identifies, analyzes, and responds appropriately to risks that may adversely affect realization of an organization's business objectives. Management's response to risks will depend on the likelihood of the event happening and the impact if it does. Based on this risk assessment, an organization will need to choose whether to accept the risk, mitigate the risk, or transfer the risk to another party. When performed effectively, these risk management activities will ensure that the organization's limited resources will be prioritized to most efficiently address the issues that will affect them the most.

Regardless of which framework your risk management program is based on, the very first step will be some form of assessing and documenting your risks. The repository of all of your active risks is what we refer to as a "risk registry". The Enterprise Risk Management Module will immediately enable you to scale beyond your existing capabilities. You'll be able to track all of the fields that you are currently tracking with a ton of flexibility to expand beyond that, with no restrictions on the number of users you can have or the number of risks you can enter. Once your risks are in the registry, you'll have access to a variety of pre-defined reporting along with a Dynamic Risk Report that gives you the ability to report on virtually any aspect of your risk management program.



Subject:

Risk Mapping: --

Category: --

Site/Location: None selected

External Reference ID:

Control Regulation: --

Control Number:

Affected Assets: Select an Asset or Asset Group

Select an Asset or Asset Group. You can create a new Asset by adding its name to the list.

Technology: None selected

Team: None selected

Additional Stakeholders: None selected

Owner: --

Owner's Manager: --

Risk Source: --

Risk Scoring Method: Classic

Current Likelihood: --

Current Impact: --

Risk Assessment:

Additional Notes:

Supporting Documentation: 0 File Added

Max 5 Mb

Tags

Complete the form above to document a risk for consideration in Risk Management Process

3. Controls Assurance & Monitoring Program:

In today's dynamic changing world, each of the organizations face an uphill task to manage the compliance requirements that are often managed in a very ad-hoc manner. Also, implementing and then managing various Systems and programs across the organization is quite a challenge. In that scenario, what we need is a Centralized Controls Assurance & Monitoring Program that addresses key features such as below:

Centralized management of control requirements for the compliances in consideration

- Structured controls repository
- Change Management for Dynamically changing compliance requirements
- Common repositories for Documentation requirements
- Mapping of Risks and Controls
- Facilitation per Audit requirements and guidelines

A common approach to managing documentation, risks and controls w.r.t Compliance requirements is the way to go as it would then act as the Single source of truth for anything to do with overall Controls Assurance and Monitoring Program across the organization.

4. Security Culture Awareness programs:

Most of the control failure we observe today within an organization is caused due to lack of security awareness and absence of education within the system. For effective governance, the organization needs to improve staff security awareness across the organization using various means. These can be broadly categorized as below:

An Effective Security Culture Awareness Program shall need to be achieved with focus on areas such as Competency Management, Resource Management, Knowledge Management etc. as can be seen below

Security Awareness Presentation (Download)

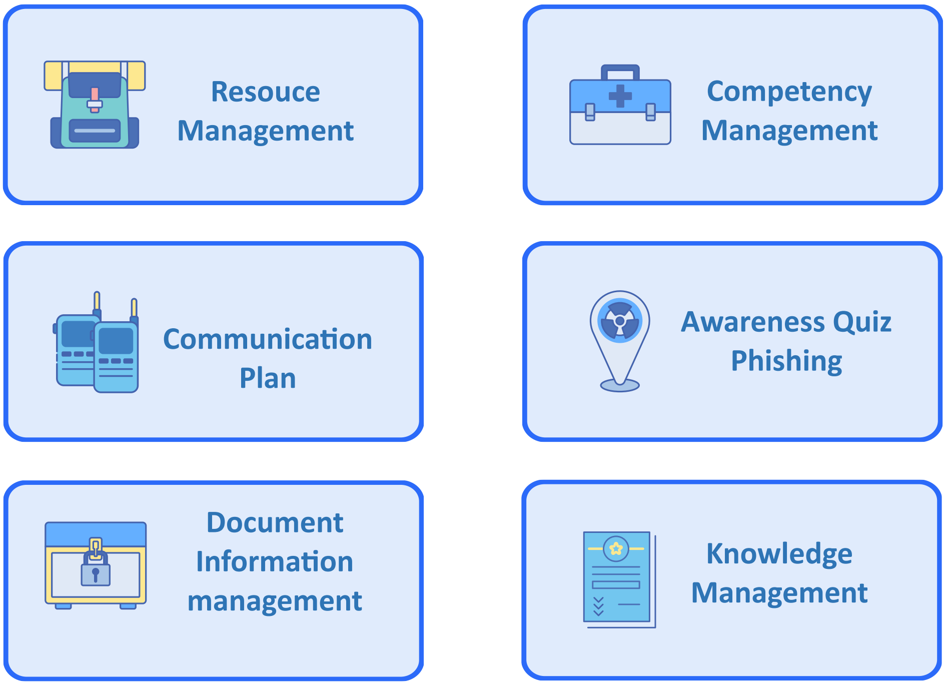
Poster (Download)

Quiz (Take a Quiz)

Phishing / Brute attack

Awareness Mail Campaign

An Effective Security Culture Awareness Program shall need to be achieved with focus on areas such as Competency Management, Resource Management and Knowledge Management etc. as can be seen below:



Resouce Management

Competency Management

Communication Plan

Awareness Quiz Phishing

Document Information management

Knowledge Management

5. Board Room – War Games:

How much ever Cyber Security Defences one has put in, an organization typically falters at the time of a crisis or an incident due to primarily the lack of information and the inability of the leaders to make the right decisions. Hence, security awareness of the Board as well as the Top Management is of prime importance as these are the key stakeholders who actually get into the War Room and provide that leadership during a crisis.

War Gaming is a scenario based warfare model in which the outcome and sequence of events affect the decision made by the players.

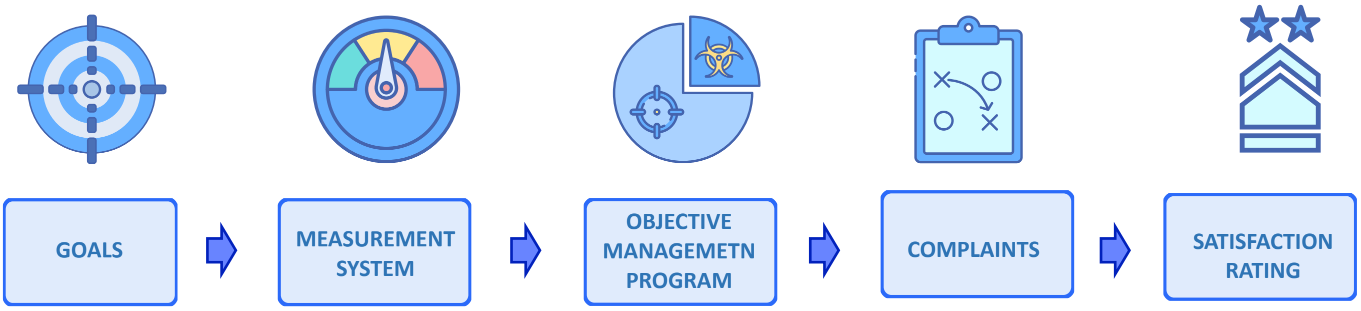
What we have built is a War Game for the Board / Top Management with real life scenarios of Cyber Security Incidents with outcomes that are impacted by the decisions of the players involved. That way, the parties get a reality check when it comes to key decision making.

This helps the team who are accountable within the system to anticipate and rehearse the steps even before it really hits them. It's a hands-on training on leadership during crisis and prepare an organization to build a robust incident management program.

The game is kept very simple and with the amalgamation of Virtual Reality into the Gamification process, a player can really experience the adrenaline rush when playing as if in real-time.

6. SOS Program Dashboards and Reporting:

Comprehensive dashboards help in effectively identifying, prioritizing and mitigating cyber security risks. This is one of the key components of the G-SOS program as it propels an organization towards enhanced Cyber Security Posture through consistent performance measurement to achieve the set goals.



SOS Program Dashboards include KPIs and Metrics for cyber risks, compliance risks, third-party risks, compliance measurement, vulnerability management, dark web monitoring, data leakage, incident management etc.

It is one comprehensive platform that provides the management with real-time insights that equips them to make the right decisions.

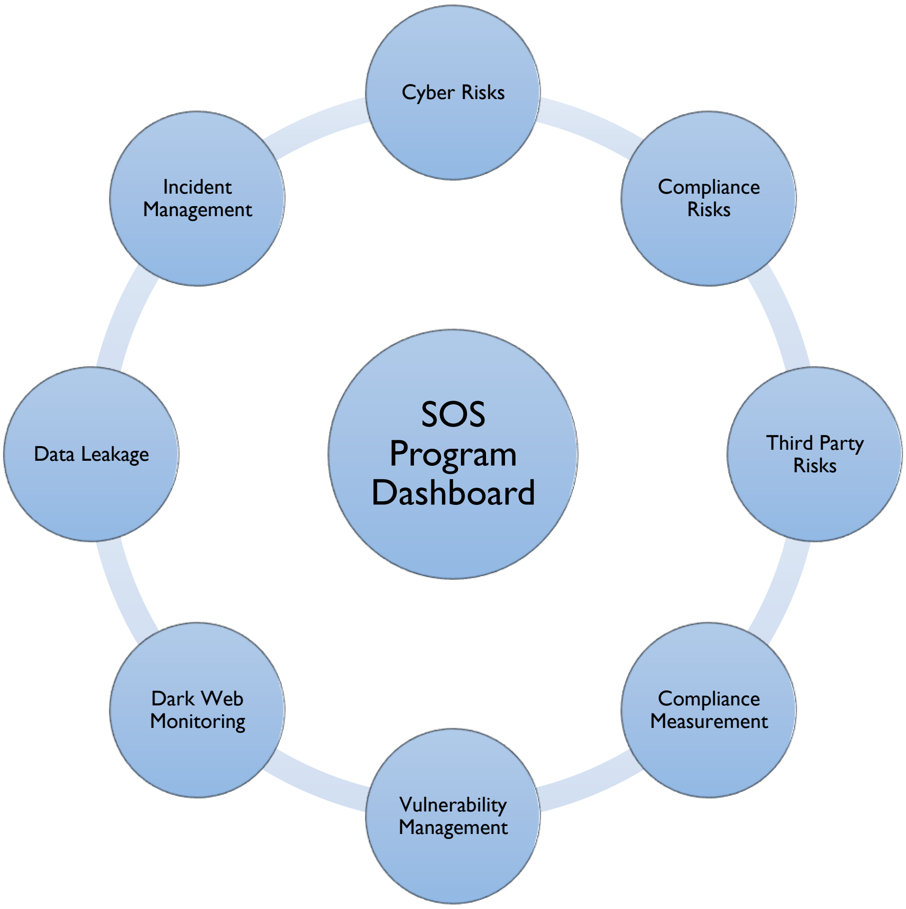


Figure 2 AI / ML Capabilities embedded within the platform help in faster aggregation and correlation of data thereby providing real-time data visualization dashboards for faster action.

Key Benefits of this Approach

The main objective of a G-SOS strategy is to establish an integrated platform to effectively establish a Governance, Risk and Compliance Framework that addresses Cyber Risks at Organization level and help the Board / Top Management make decisions on an Ongoing Basis.

This product is a strategic tool focusing on governance, strategy, risk and compliance. This board room tool provides a deep insight on the organizational structure, the vision, the mission, the existing context, the future road map, the plans supporting the strategies, the control system designed and implemented, the metrics, the dashboard, the pivotal risk management component, the communication strategy, the awareness building mechanisms, the control mapping to various international best practice standards and guidelines etc.

This is an integrated platform designed to integrate all the Compliance related best practices into everyday business processes which is indeed the need of the hour.

This platform helps to manage your entire IT landscape, infrastructure, control systems, people and creates a stronger security, risk management, assurance and compliances across the organization. This helps to streamline the operation, effective implementation of various best practice control system, governance and monitoring through a dashboard which provides the overall health of your system. It’s very correctly said “What gets monitored and measured, gets improved”.

Organizations can define their own customized control system environment, type of activity, all kinds of laws and compliance requirements based on standards, guidelines, contractual requirements which needs to be implemented internally and enforced across the organization without much pain and efforts.

This tool helps to identify and mitigate all types of risk including service delivery risk/ quality risks, security risks, privacy risks, continuity risks, technology risks, logical risks, people risks, physical and environmental risks and helps monitor company-wide strategies for risk management.

- Strategic Alignment
- Quicker Decision Making
- Streamlined Processes
- Simplification & Gamification
- Goals & Measurement
- Build a Security Culture
- Optimization of resources
- Enhanced Cyber Security Posture

Way Forward

This Integrated Platform is a One-Stop Solution for effectively managing Cyber Security Risks across the organization. The seamless integration it achieves along with the organization wide Cyber Security Strategy and the Governance, Risk and Compliance program is a highly evolved and holistic approach to identifying, prioritizing and mitigating Cyber Risks. Quick decision making prowess it provides the Company Board and the Top Management is unheard of and unmatched. This strategy is going to Strengthen the Organization from within and provide a strategic direction that is evolved and in line with today’s dynamic and ever changing world.

This approach is an integrated plug-and-play model that seamlessly fit into your Cyber Program and enhances the overall Cyber Security Maturity of the organization.

About Infopercept - Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Imprint
© Infopercept Consulting Pvt. Ltd.

Created Date
Sep 2023

Contact Detail
sos@infopercept.com
www.infopercept.com/whitepapers