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 Cyber Risks in a way that is aligned with the overall strategic direction of the company.

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,
- Centralized Control Assurance & Monitoring Program and
- Organization Wide Awareness Programs.
- 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.

At Infopercept, we address this requirement through **G-SOS** (Green- Secure, Optimize and Strengthen) Strategy.
This obviously leads to security breaches & consequently individuals coming to us to get them out of this critical security and protect them.

We call it the SOS situation in which the person only really pays attention to their security health when it is already compromised. In line with our aim to always provide solutions to our clients we devised a Green - SOS (Security Optimize & Strengthen) to counteract the breach SOS.
Current Cyber-Strategy Landscape Shortcomings

**SHORTCOMINGS**

- **Governance**
  - Very Complex Solutions and Clarity Missing
  - Solutions: Simplification and Gamification

- **Risk**
  - More need driven to meet compliance requirements
  - Solutions: Simplification and Interactive

- **Compliances**
  - Various Compliances with no integrations. More of a burden then a wish.
  - Solutions: Simplification and Mapping of requirements

- **Tools and Technology**
  - After doing huge investment still not clear on use cases
  - Solutions: Simple Direction on Use Cases
Current Cyber-Strategy Challenges

CHALLENGES

- Lots of Information
- No KRA/KPI
- No Team Work
- Real Time

SOLUTIONS

- Slicing and Dicing of Data to have proper actionable. Mapping requirements
- Gamification and Simplification to encourage participation
- Cyber Security Team Activities to drive accountability culture
- Strategy requires peaceful thinking. Gamification to understand risk have proper strategy
Multiple Standards to comply

Central Banks’ Req.
Respective Cyber Security Framework

ISO 27001
Information Security Management System

ISO 20000
Services Management Systems

ISO 22301
Business Continuity Management System

SWIFT
SWIFT CSP

ISO 31001
Risk Management Systems

NIST
NIST 800-53

PCIDSS
Payment Card Industry Data Security Standard
Multiple Points Technology

- Intrusion Detection
- Encryption
- Anti-virus
- Network Access Control
- Identity management
- Content Filtering at Gateway
- Converged Desktop Security
- HIPS
- Patch Management
- Anti-Spyware
- Biometrics
- Firewalls
- Background Verification
- Access Control
- Personal Firewalls

"Infopercept Proprietary Material - Please do not copy or distribute"
Introducing Invinsense G-SOS

Click Green SOS Button

PEOPLE
• Staff training & awareness.
• Professional skills & qualifications.
• Competent Resources.

SECURE
• Management Systems
• Governance Frameworks
• IT Audit

PROCESS

GREEN SOS

TECHNOLOGY

OPTIMIZE
• You can’t deploy technology without competent people, support processes or an overall plan.

STRENGTHEN

"Infopercept Proprietary Material - Please do not copy or distribute".
We are using Green (Proactive) Secure; Optimize and Strengthen as a Strategy that cuts across People, Process and Technology paradigm.

G-SOS

**SECURE** system components

Design system components

**OPERATE AND OPTIMIZE** system components effectively

Monitor and measure

Improve and **STRENGTHEN**

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

G-SOS platform consists of the following 6 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.
2. Enterprise Risk Management

- 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.
- 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.
3. Controls Assurance and 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:

- Security Awareness Presentation (Download)
- Posters (Download)
- Quiz (Take a Quiz)
- Phishing/Brute attack
- Awareness Mail Campaign
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.
Benefits of Invinsense G-SOS

- Strategic Alignment
- Quicker Decision Making
- Streamlined Processes
- Simplification & Gamification
- Goals & Measurement
- Build a Security Culture
- Optimization of resources across levels
- Enhanced Cyber Security Posture
By accessing/ proceeding further with usage of this platform / tool / site / application, you agree with the Company’s / Infopercept Consulting Pvt. Ltd.’s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions, kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Your Ally in Digital Warfare!