

Gemini Communication Ltd.



Four S

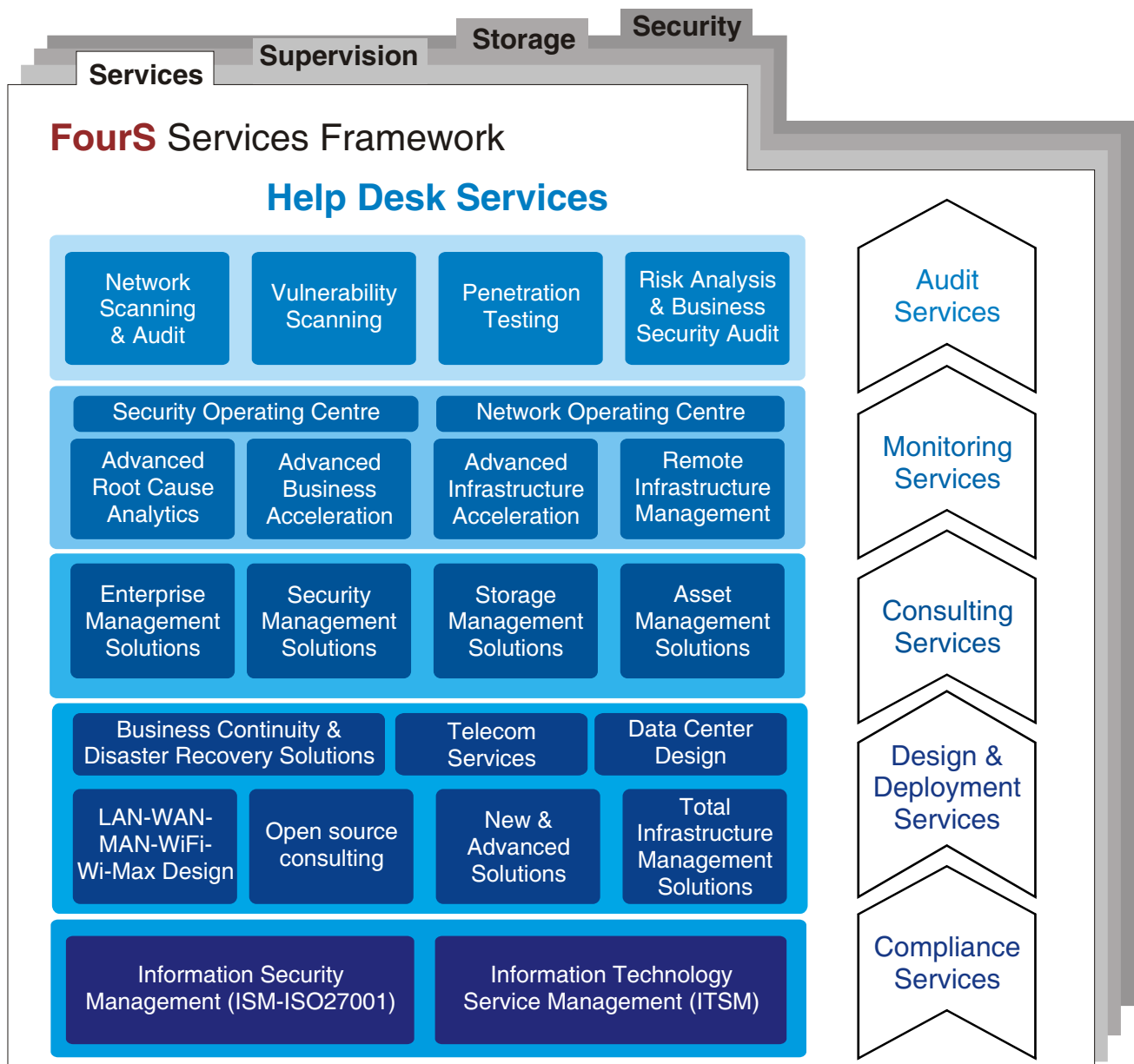
Security Storage Supervision Services

FourS Services Framework

- ❖ FourS services framework is a product of best practices from Gemini in the Information Technology space and system integration space over the last ten years.
- ❖ Gemini's initiative of documenting its implementation experiences has matured into the seamless Services Framework.
- ❖ Gemini Offers the best of breed flexible IT services to suit the needs of all tiers of industries.

Key Benefits

- ❖ Gemini's Services Framework goes by an holistic view on your organization to determine the impact of Design, IT Infrastructure, security and compliance failure on your operations, your reputations and your business objectives.
- ❖ Using industry best practices, Gemini helps you to develop effective business continuity strategies and customized solution to meet your recovery time and recovery point objectives.
- ❖ Simplicity of approach and flexible service level agreements (SLAs)



Reduce desk side visits : Improve Asset Inventories

Remote Infrastructure Management (RIM)

Network Monitoring: Gemini FourS monitors networks and performs basic event recognition and logging. Upon recognition of an alarm or alert, FourS Surveillance Technician will notify the customer of the condition. Additionally, Gemini FourS will field trouble calls from the customer's technical staff, answering incoming calls on a private line from customer technicians to address trouble reports and provide other relevant information.

Device Management: Device monitoring applications include availability, health and utilization statistics of backbone, core and customer premise devices.

System Device Monitoring applications includes availability, health and network interface utilization statistics of devices. It also includes application-level resource utilization for specific operating systems.

Event Aggregator consolidated view of alerts generated by all systems with visual and audible cues based upon incident severity

Trouble Ticketing - severity and priority tracking of all proactive and reactive incidents with daily, weekly and monthly exception reporting.

Vendor Management: Implementing the vendor management function is the most

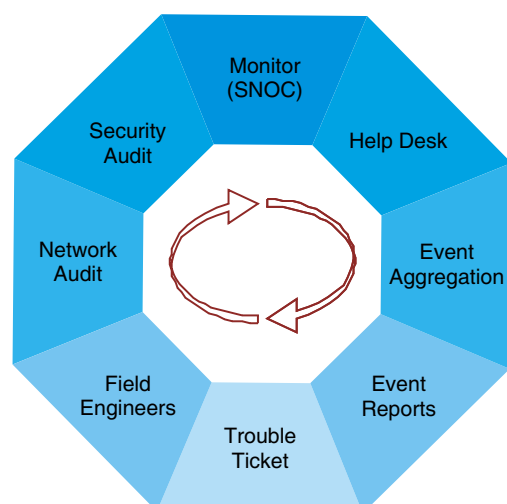
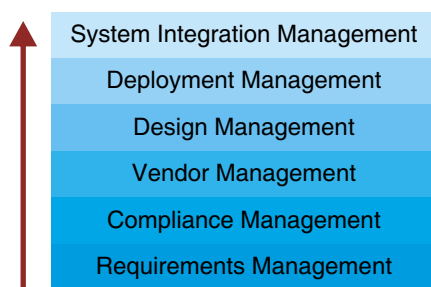
efficient means of reducing IT cost, basically through consolidation of vendors, application of greater buying leverage, and the use of more sophisticated techniques for managing vendors.

RIM Features

- ❖ Network Monitoring
- ❖ Asset Inventory
- ❖ Device Management
- ❖ System Device Monitoring Applications
- ❖ Remote Problem Resolution
- ❖ Event Aggregator
- ❖ Trouble Ticketing
- ❖ Vendor Management

RIM Benefits

- ❖ Monitoring all backbone links and network devices
- ❖ Ensuring continuous operation of servers and services
- ❖ Providing quality support for corporate customers
- ❖ Troubleshooting of all network and system related problems
- ❖ Opening tickets to track and document resolution of problems. 24 hours a day, 7 days a week supervised operation by highly skilled network and system engineers.



Shift your focus from managing PCs to accelerating Business

Vulnerability Assessment & Penetration Testing

In computer security, the word **vulnerability** refers to a weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system or the data and applications. Vulnerabilities may result from bugs or design flaws in the system. Vulnerabilities have been found in every major operating system including Windows, Mac OS, various forms of Unix and Linux, OpenVMS, and others. Vulnerability may allow an attacker to misuse an application bypassing access control checks or executing commands on the system hosting the application.

The only way to reduce the chance of a vulnerability being used against a system is through constant vigilance, including careful system maintenance (like updated software patches), best practices in deployment and auditing throughout the deployment life-cycle.

Corporates are advised to go for a periodical vulnerability audit at least twice a year. There are two types of vulnerability audit depending on the location from which the audit is being carried out.

Internal vulnerability assessment is carried out with in the LAN environment. The scope of the assessment includes assessment of the servers and other network gadgets. The assessment is carried out without the intervention of firewall.

External vulnerability assessment is done outside the LAN. The assessment is primarily carried out to check the status of the firewall deployed. It helps in identification of information leakages through the permitted ports in the firewall and application level security issues seen through the firewall.

Methodology

The audit team will collect the IP addresses of the servers which require an audit to be carried out. The auditor runs his set of tools on the collected network addresses. **Pre vulnerability assessment** is carried out to assess the status of the naïve servers. Based on the vulnerability assessment report, selected vulnerabilities are identified for penetration testing leading to proof of concept. Once the identified vulnerabilities are closed a **Post vulnerability assessment** is carried out as a validation exercise. The post scan is equally important from the angle of ensuring closure of vulnerability issues.

Tools

A variety of tools are available in the market. The team works on a combination of two optimally selected tools for the purpose of validation of reported exploits and for the purpose of ranking the exploits. The team heavily depends on Nessus and substantiates the results with other commercial tools.

Knowledge Base

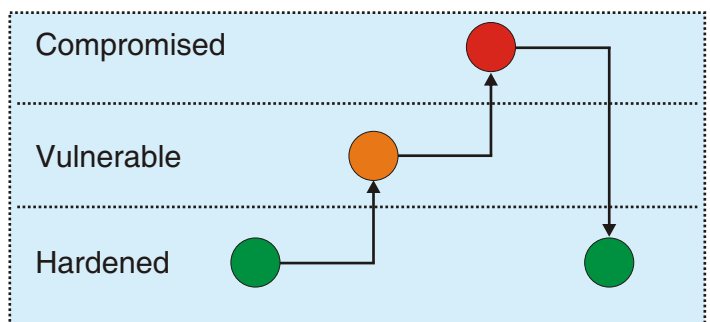
Auditors with understanding of host lifecycle have updated their knowledge levels on vulnerability status of hosts. The lifecycle starts with the birth, discovery, disclosure, correction, publicity and death of potential vulnerabilities. The public forums, National and international databases are the primary source of knowledge update. The update is important to keep the knowledge level abreast.

Deliverables

- The deliverable would be a comprehensive report on the status of vulnerabilities of the servers audited. The report includes audit findings in diverse areas as indicated in the table below.

UDP	User Accounts
TCP/IP	Telnet/FTP
Registry	DNS/Web servers
VPNS	POP3/SMTP/IMAP
Routers	Application Servers
Windows/Linux	Database Servers
SNMP	DOS Vulnerabilities
Sql Injection	Proxy
CGI Scripts	SSH/SSL

The report will include recommendations on vulnerabilities.



Network Audit (NA) Wired & Wireless

Network Audit

Gemini's Audit team will analyze the network environment and provide details on the condition of network. The deliverable includes a summary report highlighting conditions that require further diagnosis or immediate resolution, with suitable recommendations on course of action.

Network Audit and Analysis provides an Assessment of Network's Performance.

Benefits

- Help optimize existing network components
- Pro-actively identify and resolve traffic and design issues.
- Increase network performance and availability.
- Establish baselines to measure future improvements or changes
- Better optimization of all IT resources
- Pro-actively reveal potential trouble areas
- Identifies corrective actions
- Identify areas for improvement for optimum performance
- Maximizes system availability and accessibility for enhanced end user

Productivity

- Maintains reliable system performance guards against degradation overtime.
- Reduces network management costs by reducing the time required to collect and diagnose system data.

Methodology:

Pre-Audit:

Initial information collection and validation is carried out in this phase. Network Auditors collect critical inputs and data, validate the collected information for developing a detailed project plan. The deliverable of this phase is an audit implementation plan.

Audit:

Audit professionals establish the current state of client/server infrastructure by performing a physical audit of network infrastructure, followed by a logical audit of network traffic (including utilization, performance, errors and traffic patterns). Network Audit team conducts an operations audit for capturing information on relevant processes, procedures and supporting documentation.

Analysis:

Gemini employs a structured process for auditing networks, with the most sophisticated network auditing tools available. Guided by Audit's structured analysis methodology, all of the audit information gathered is analyzed to identify opportunities to improve your network. Audit experts consider internal factors – corporate strategies, organizational issues, technical biases etc – as well as external factors like competitive pressures, new technologies and pertinent standards.

Recommendations:

Delivered in a formal report, Audit summarizes objectives, reviews all findings and clearly identifies recommendations to improve your network's performance.

Report will Include Analysis of:

Network Configuration – Includes networking physical configuration and software logical configuration, network configuration and overall environment as it relates to your existing network.

1. Pre-Audit Summary
2. Existing Network Schematic Diagram
3. Understand problems Identified by the customer
4. Evaluation of the Physical Layer Infrastructure
5. Evaluation of Data Link Layer Health
6. Evaluation of Network Layer Health
7. Identification of Network Problems
8. Documentation
9. Recommendation for solving problem identified during Audit
10. Suggestions to optimize Network for Future expansion
11. Existing Network Diagram
12. Proposed Network Diagram
13. Conclusion
14. Physical Layer Test Summary Report



Shift your focus from managing PCs to accelerating Business

Security Network Operation Center (SNOC)



As the enterprise IT environment becomes more geographically dispersed and the number of remote users increases, the need to manage and support these vital business resources

from afar becomes crucial. If remote resources are not managed quickly, efficiently and reliably, business performance may not reach its potential.

Security & Network Operating Center (SNOC) is a state of art division equipped with latest applications and monitoring tools, functional in Chennai, Gemini Communication Ltd. SNOC is used for monitoring the network based on service level agreements(SLAs).

Delivery

Gemini SNOC leverages its services delivery architecture to securely deliver services to quickly improve and maintain the performance and availability of Network and their infrastructure. For the most secure problem resolution, Gemini SNOC has created Technology Teams, which are teams of IT experts versed in Network troubleshooting and management problems. Our Technology team works on 24x7 basis from our NOC at Chennai, India and exclusively focus on basic administration and problem resolution. For every technology team, there will be a technology manager who coordinates, troubleshoots and manages all activities to ensure the fastest time to resolve any issue.

Gemini SNOC system administration, incident and problem resolution processes are framed on IT Service Management Best Practices (ITSM) principles. Gemini SNOC embraces ITIL best practices, enabling organizations like yours to optimize IT services in their complex environments to effectively deliver the value of an on-demand infrastructure.

Network Operations Management

- Remote IT Infrastructure maintenance
- Real-time monitoring of critical equipments
- Critical WAN Link Monitoring
- Network Device Health Check
- LAN Monitoring
- Configuration Management
- Network Documentation
- Root Cause Analysis
- Network usage trending and planning
- Help desk

Server and Application Management

- Server Management Service
- Server Administration for Windows and Linux flavours, Support for Domain Server, DNS and DHCP Servers.
- Web server Management Service
- Support for IIS, Tomcat, Apache Web Servers
- Server Load Balancing for better end user performance
- Secured Access for Resources in a Portal Environment

Secure IT

- Build and Maintenance of IT Security Infrastructure
- Desktop Antivirus and Antispyware
- Gateway Antivirus
- Firewall
- Server OS Hardening
- Content Filtering
- Anti Spam
- Security Patch Management
- IDS and IPS



Reduce desk side visits : Improve Asset Inventories

FourS Gemini Managed Security Services & Monitoring Services

Firewall is deployed by organizations to safeguard their internal network. The complexity of a firewall is well understood by a firewall specialists. Firewall specialist deploy rules to safeguard their LAN from attackers. They also ensures that firewall rules do not stale over time. Firewall specialist reads logs and dynamically readjusts his firewall policy settings to take care of changing faces of Internet and Internet induced threats. Understanding this dire need, Gemini true to its commitment “**Leave IT to Us**” provides security services through Gemini Managed Security & Monitoring Services.

Gemini Managed Security Services

Updated firewall Rules:

Rules are statements written into Firewall Box to monitor the incoming and outgoing IP packets. The action taken on the packets are logged to identify potential attacks, IP attack, denial of service or Masquerade. Rules are built on the protocol types. Application of appropriate rules stops unnecessary traffic in the network. Gemini's SOC team deploys new policies based on the registered log and traffic patterns. [Version control of applied rules to enable role back.](#)

Rules need to be version controlled and documented. Version controlled rules act as backup of the firewall policies thereby providing business continuity. Gemini's SOC team document each and every rule applied to the box.

24X 7 X 365 Watch on Firewall and its operation.

To pro-actively detect and respond to attacks 24X7 monitoring becomes imperative. Deployment of required experts for a 24X7 monitoring involves a huge cash outflow for organizations. Gemini equipped with the right team extends a marked reduction in cash outflow for organizations.

Reporting & Documenting Events.

In-house reporting tools provided limited or no visibility into the security infrastructure. Reporting becomes extremely crucial for forensics and analysis. A forensic activity demands a log analysis for specific traffic pattern from an organization. Gemini today can store the log of organization for a

specified period of time. Older logs are removed unless specified by the customer.

Powerful Event Correlation

In a corporate event handling activity is people dependent. Due to fuzzy event occurrences, it becomes difficult to co-relate similar incidents to detect an attack. GMSS & GMMS practices automated event co-relation capabilities that list events with similar patterns to detect attacks.

Trained & Dedicated Professionals

Dedicated Certified security professionals undergo periodical knowledge and skill up gradation to tackle security emergencies. They equip themselves with the current vulnerability and threat listings as reported world wide.

Guaranteed Responsiveness

GMSS & GMMS begins escalation the moment a problem is detected and the source is identified. Aggressive SLAs ensure that organizations are notified.

Managing False Alerts

99% of security alerts are made of false positives. A typical firewall generates thousands of alerts daily and the sheer volume of logs generated becomes an issue for the organization. GMSS & GMMS has automated tools that segregate the 1% of actual attacks.

Weekly reports on Intrusion Attempts and trend analysis

Weekly reports on “aggregated gateway traffic” pertaining to the client's firewall are prepared. The prepared reports are cross verified by the Manager, SOC and the passed for dispatch to clients address.

Event Reports

Various Reports are generated

Telnet Usage reports	Traffic Report
Streaming & chat reports	Protocol usage reports
Firewall Rules reports	Web usage reports
FTP usage reports	Attack reports
Traffic Trend reports	Security Reports

Shift your focus from managing PCs to accelerating Business

Data Center Design (DCD)

Data center is a centralized location for storage management processing and exchange of data that exist within a specific enterprise. Most of the business units have recognized that data is their biggest asset. Business obligations are forcing IT departments to ensure that their availability and disaster recovery systems are sufficient to comply with demands and standards.

Data centers are equipped with high speed high demand networking communication systems capable of handling network traffic for SAN, NAS , File, application and web server forms.

The challenges include the control of humidity, electrical controls, fire controls, floods, data reliability, etc for the purpose of business continuity. It also includes managing higher densities, cable management and heat control. Moreover, as computing density increases in the data center, a corresponding increase in equipment exhaust temperatures occurs. Inside each rack, an inadequate supply of chilled air may result in the consumption of used air; some equipment may consume air from its own.

Data center generally has an entrance room that contains service provider demarcation area points and equipment and a main distribution area (MDA). MDA houses core switches and serves as the central connection point. The data center one or more horizontal distribution areas (HDA). HDAs connect equipment distribution areas. (EDA). A consolidation point is planned to serve the equipment distribution area called as Zone distribution area (ZDA).

General Benefits

- Initial investment protection
- Standards based open systems
- High performance and high bandwidth
- Support for 10G & high speed technologies
- Support for storage devices (SAN /NAS)
- Support for convergence
- High Quality, Reliability and Scalability
- Redundancy & Path diversity
- High capacity
- High Density

Data center racks and equipment can take up an enormous amount of real estate, and the future demand for more network connections, bandwidth and storage may require even more space. A data center cabling design is different from normal commercial building cabling design.

Gemini's Strength

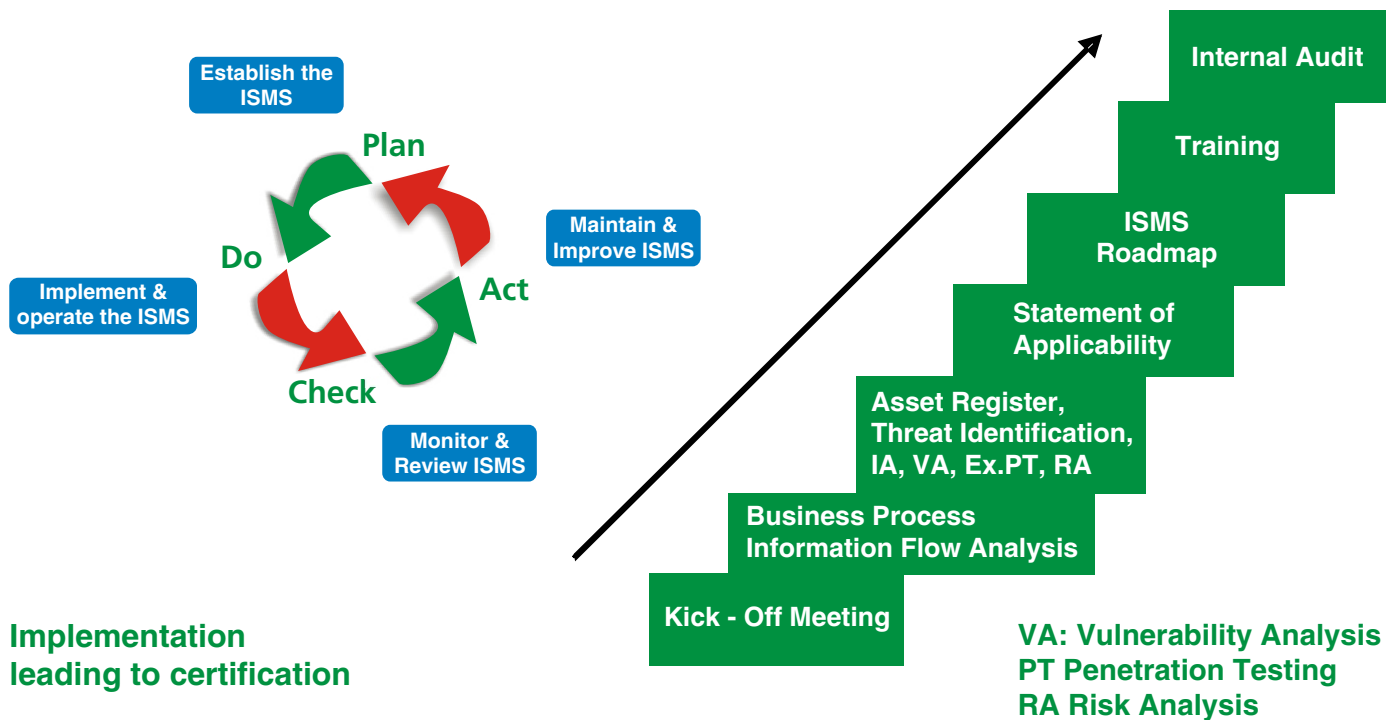
Gemini's inherent strength of system integration over the years has consolidated Gemini's position in the areas of Data center design. Gemini has the right blend of design engineers capable of working on design requirements.

Engineers believe in standards approach and build the design on standards thus providing the requisite scalability, interoperability and protect initial investments.

Knowledge up-gradation

Gemini strongly believes in knowledge community and motivates all its employees to take up advanced insights into technology.

Information Security Management Systems



Security Practices [SP]

The first and foremost guideline for us is our values and principles. Our consultants are committed to integrity and honesty. This is of paramount importance considering the line of our work, leading to trust & well cemented relationships. The business activity, naturally, comes from a strong adherence to these core values.

ISMS provides recommendations for information security management. It is important for those who are responsible for initiating, documenting, implementing or maintaining security in their organization. ISMS also specifies requirements for establishing, implementing and documenting information security management systems.

Subject Matter Expertise (SME)

We possess the right blend of senior level experience and in-depth technical know-how to be able to carry out a security audit and assessment exercise that exceeds your expectations.

Standards Based Approach (SBA)

We follow the universally accepted standards for security (COBIT) (ISO27001)(ITIL). The audit approach is designed to cover all aspects of security including People, Processes and Technology.

Our team consists of certified lead auditors and implementation experts with the right blend of technical and business process know how. Our focus is always on the triad People Process and Technology

SBA enables an organization to put in place a documented ISMS which complies with the requirements of the standard. SBA helps the organization to assess its risks through a management decision process to establish and implement a sound system of controls to manage its risks which includes implementing processes for monitoring and reviewing the effectiveness of ISMS and for continual improvement

Vulnerability Scanning [VS] & Penetration Testing (PT)

An expert team of vulnerability scanners & penetration testers with cognizance in widest variety of technologies are a part of ISMS division. Vulnerability scanning & penetration testing exercises were carried out by us for a wide range of clients

Benefits

Lower Cost of ownership
Leveraging Expertise
Ensuring high levels of service
Tide over IT attrition Problem

Meet Critical
IT Challenges
With
Gemini FourS

- At a Glance
- Network Architecture Design
- Wireless Architecture Design
- Security Architecture Design
- Network Audit & Reporting
- Penetration & Vulnerability Assessment
- Managed Secure Monitoring (Platinum, Gold & Silver)
- Managed Device Configuration, Device Management and Monitoring
- Managed Total Protection & Prevention Services (ISO27001)
- Managed Firewall Services (including Virus & SPAM)
- Managed Intrusion Detection Services (IDS)
- Managed Virtual Private Service Networks
- Security Training as per ISO27001
- Managed Telecom Services (Platinum, Gold & Silver)

REGISTERED OFFICE

Gemini Communication Ltd.

#1, Dr. Ranga Road, 2nd Street, Alwarpet, Chennai -600 018

Phone: 91-44-2499 6422

Fax: 91-44-2499 5062

E-mail: info@gcl.in, URL: www.gcl.in

GEMINI
Leave IT to us