Assurance & Compliance Unit

The Assurance & Compliance Unit within STS Security Department is dedicated to managing information-related risks and safeguarding information systems. Our primary objective is to ensure the confidentiality, integrity, and availability of information and information resources while maintaining full compliance with Information Security Management regulations and standards.

Our Information Assurance Services are designed to oversee the information security program comprehensively. This includes:

- **Confidentiality:** We implement measures to ensure that sensitive information is accessed only by authorized personnel and remains protected from unauthorized access or disclosure.
- **Integrity:** We employ mechanisms to ensure the accuracy and reliability of information by preventing unauthorized modification or deletion.
- **Availability:** We work to ensure that information and information resources are accessible to authorized users whenever needed, while mitigating the risk of downtime or disruptions.

We manage the security activity, provide security assessments, audits, awareness & GRC Services

GRC services provided by our unit encompass a set of processes and procedures based on security best practices, national, and internal standards. These services are tailored to help organizations achieve their business objectives while effectively managing risks. Key components of our GRC services include:

- **Governance:** We establish frameworks and mechanisms for decision-making, accountability, and oversight related to information security.
- **Risk Management:** We identify, assess, and prioritize risks to information assets, and implement controls to mitigate these risks effectively.
- **Compliance:** We ensure adherence to relevant laws, regulations, and industry standards, as well as internal policies and procedures, through comprehensive compliance programs and monitoring mechanisms.

By leveraging our expertise and resources, organizations can enhance their resilience to information-related risks and demonstrate their commitment to maintaining the highest standards of information security and compliance.

Main Services Under Assurance & Compliance Unit

A&C Services	Description
GAP Assessment Service	Comprehensive evaluation conducted to identify gaps or weaknesses in an organization's existing security measures, policies, and practices. The primary goal is to assess how well an organization's security posture aligns with industry best practices, regulatory requirements, or its own security objectives.
Risk Assessment Service	A systematic process designed to identify, analyze, and prioritize potential risks to an organization's information assets, systems, and operations. The primary objective is to understand the likelihood and potential impact of various threats and vulnerabilities, allowing the organization to make informed decisions about how to mitigate or manage those risks effectively.
Information Security Policies & Procedures	Helping organizations to develop comprehensive and tailored set of policies, standards, guidelines, and procedures to govern the management, protection, and use of their information assets
National Security Compliance Management	The process of assuring that the organizations Information Security Controls, processes, plans comply to regulations & standards such as: • SAMA Regulations: SAMA created a cybersecurity framework to identify appropriate measures to efficiently detect and resolve cybersecurity issues. With the establishment of a Cybersecurity Framework, regulated companies are supported by the development of adequate cybersecurity governance, a robust infrastructure, and the investigative and preventative measures necessary. • NCA Essential Cybersecurity Controls (ECC): The NCA ECC was developed to ensure organizations maintain and support the Cyber Security initiative to protect the interests, national security, critical infrastructure, and government services. It was developed with an aim to set minimum Cyber Security requirements for information and technology assets in organizations of Saudi Arabia. • CBJ Regulations: The CBJ sets standards and requirements for information security within financial institutions to protect sensitive customer data, prevent unauthorized access, and mitigate cybersecurity risks.
Security Awareness Training	Is designed to educate users on the appropriate use, protection and security of information, individual user responsibilities and ongoing maintenance

	necessary to protect the Confidentiality, Integrity, Availability, Accountability and non-repudiation of information assets, resources and systems from unauthorized access, misuse, disclosure, destruction, modification, or disruption.
International Standards Compliance Management	The process of assuring that the organizations Information Security Controls, processes, plans comply to International Standards such as: ISO27001 (ISMS): is the international standard for information security. It sets out the specification for an information security management system (ISMS). ISO27001 helps organizations establish, implement, operate, monitor, review, maintain and continually improve an ISMS by addressing people, processes, and technology.

Offensive Security Unit

At STS Offensive Security Unit (OSU), we focus on proactively identifying and exploiting vulnerabilities within the organization's systems and networks to strengthen defenses and prevent potential breaches. Our team of skilled professionals employs a variety of cutting-edge techniques and tools to simulate real-world attack scenarios, providing valuable insights into weak points that adversaries could exploit.

The primary objective of our diverse services is to assess the security posture of the organization by identifying and exploiting vulnerabilities before they can be exploited by malicious actors. Through a combination of automated scanning, manual testing, ethical hacking, and social engineering, we uncover potential weaknesses in networks, applications, infrastructure, and people providing actionable recommendations for remediation.

Operating with precision and employing a range of testing methodologies including white box, black box, and grey box tests, the OSU conducts thorough assessments to evaluate the organization's security posture. White box testing provides an in-depth analysis of internal systems and structures, while black box testing simulates attacks from an external perspective, and grey box testing combines elements of both approaches for a comprehensive assessment. This approach allows us to uncover vulnerabilities from various angles and enable tailored recommendations.

Testing Type	Description
White Box Testing	The tester has full access to the internal workings and source code of the system or software.
Grey Box Testing	The tester has partial knowledge of the system, typically access to limited information or some internal details. Such as: Defined IP's.
Black Box Testing	The tester has no prior knowledge of the internal workings or source code of the system.

By engaging our extensive services, organizations can proactively identify and mitigate risks, safeguarding their assets and reputation. Our comprehensive reports outline identified vulnerabilities, their potential impact, and actionable recommendations for remediation, empowering organizations to strengthen their security posture effectively.

Main Services Under OSU

OSU Services	Description
Vulnerability Management Service	Establish processes and procedures for identifying, prioritizing, and remedying security vulnerabilities across the organization's infrastructure to reduce risk exposure.
Vulnerability Scanning Service	Automated scans of networks, systems, and applications to identify potential vulnerabilities that could be exploited by attackers.
Vulnerability Assessment – Security Assessment Test Service	At OSU we conduct comprehensive evaluation of systems, applications, and networks to identify known vulnerabilities and prioritize remediation efforts based on risk.
Essential Cybersecurity Checks Service	Our team performs basic checks to mitigate the risk of unauthorized access to critical systems ensure that systems are properly configured due to poor configuration.
Penetration Testing Service	OSU Simulates Internal/External attacks on systems, applications, or networks to identify and exploit vulnerabilities and assess the effectiveness of security controls and, if applicable, incident response procedures.
Physical Bypass Service	When it comes to physical bypass our team studies the scope that has been provided by the client and produce tailored scenarios to bypass physical security, attempting to bypass measures such as access controls to gain unauthorized access to sensitive areas or assets.
Wireless Penetration Testing Service	Assessment of wireless networks and devices to identify security vulnerabilities such as weak encryption, misconfigured access points, and rogue devices.
Network Penetration Testing Service	Involves simulating attacks on the organization's network infrastructure to identify weaknesses, misconfigurations, and vulnerabilities that could be exploited by attackers.
Web Application Penetration Testing Service	Our team Focuses on assessing the security of web applications by attempting to exploit vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms, adhering to OWASP Top 10.
Security Application Testing (Mobile App) Service	Specialized testing for mobile applications, to identify security vulnerabilities that could compromise the confidentiality, integrity, or availability of data.

Static Application Security Testing (SAST) Service	Analyze the application source code or compiled version of an application, SAST tools scan the code for potential security flaws, such as SQL injection, cross-site scripting (XSS), or insecure cryptographic implementations, adhering to OWASP Top 10.
Dynamic Application Security Testing (DAST) Service	Assess the security of a running mobile application by sending various requests and inputs and studying responses to identify potential vulnerabilities. Unlike SAST, DAST evaluates the application in its runtime environment, providing insights into how it behaves under real-world conditions. Which helps uncover vulnerabilities that may not be apparent in the source code alone.
Phishing Campaign Service	Simulate real-world phishing attacks to evaluate the susceptibility of employees to social engineering tactics and assess the effectiveness of security awareness training.
Configuration Review Service	Review and assessment of system configurations, including operating systems, network devices, and applications, to ensure compliance with security best practices and industry standards.
Source Code Review Service	In-depth analysis of the source code of applications to identify security flaws, coding errors, and potential vulnerabilities that may not be apparent through other testing methods.
Stress Testing Service	Evaluation of systems or applications under high loads or adverse conditions to assess performance, stability, and resilience against potential attacks or failures.

Cyber Threat Investigation Unit

Whether facing acts of cyber fraud, identity theft, government investigations or regulatory inquiries or major litigation, you should turn to **STS - CTI** Unit for assistance.

Cyber Threat Investigation Unit within STS security department will investigate threat events detected in our client environments by conducting **RAM Analysis service** and **Computer/Disk analysis service**, deliver high quality reports to our clients, support client's teams on remote sites, working closely with their own security incident management elements and support the delivery of long-term cyber threat investigation projects, both on site and remotely. Where necessary, we may also deploy to client sites to undertake cyber related investigations.

Pro-active Cyber Investigation aims to:

- Cyber Threat hunting and Breach Detection service to make identify whether systems in scope are breached or not.
- Acceptable Use Policy violation by employee(s) for the systems in scope of (Computer Investigation).
- Tool Analysis service (detecting hacking tools, spyware software, …etc) for the systems in scope.

RESPONSIVE CYBER INVESTIGATION SERVICE, ONLY BY STS

This service enables you to request the cybercrime investigator accredited in our company to begin a responsive electronic investigation only in the event of the existence or discovery of a cybercrime. In other words, the cybercrime must have occurred in order to begin this service on our part.
Electronic forensic analysis service (responsive investigation) and its benefits:
1. Providing a certified electronic forensic investigator to follow up on the electronic crimes that have occurred.
2. A 12-month subscription in the event of a cybercrime, up to a maximum of 12 cybercrimes.
3. Immediate response to cybercrime to stop it and analyze it to identify its perpetrators if possible.
4. Providing solutions and advice to avoid repeating the cybercrime that occurred. To achieve response to cybercrimes.

When should we subscribe to the electronic forensic analysis service? Responsive investigation?

- In the event of a history of electronic sabotage, ransomware, data erasure, or intentional electronic sabotage by employees.
- If the company's management suspects that there is strange activity on the company's computer systems and/or mobile phones.
- At STS, we advise all companies to adopt a company specialized in investigating electronic crimes.

What types of cybercrimes fall within the Cyber Threat Investigation Unit?
A- Tracking electronic attacks on the company's website or financial systems.
B- Ransomware attacks that encrypt information.
C- Electronic attacks targeting the company's financial department systems.
D- Leaking of sensitive and company-specific information by a hateful employee.
E- Analyzing electronic intrusions targeting the company's email.
F- Evaluating the damage resulting from electronic attacks.

Main Services Under CTIU

CTIU Services	Description
Responsive Cyber Forensics Service	**Responsive cyber forensics service** is an advanced security service offered by STS cyber threat investigation unit, where this service enables you to request a certified and accredited cyber forensics examiner from STS to initiate the investigation in the event of the existence or discovery of a cybercrime, in other words, the cyber-criminal act or suspect **must** occur in order to start this service.
Proactive Cyber Forensics Service	**STS** Proactive cyber investigation will acquire a sample of network traffic, computer images, and RAM Images in order to analyze and investigate any potential breaches.

RAM Forensics service	This service aims to detect if a computer is breached and exfiltration data outside, certain advanced malware is not detected by security controls and able to hide their operations and remain hidden, STS RAM forensics service will create a forensically sound image of the RAM and analyze it in order to detect any weird connections and/or rogue processes.
Physical Bug Detection Service	Inspection and testing of physical infrastructure, devices, and equipment to identify security vulnerabilities, weaknesses, and potential points of entry for attackers.
IOS Spyware Detection Service	Detection and analysis of spyware, malware, or other malicious software targeting mobile devices to protect against unauthorized access and data theft.

Security Managed and Implementation Services Unit

The Security Managed and Implementation Services Unit (SMI) within the STS security department is a dedicated team committed to ensuring the comprehensive security of the organization's and customers' digital infrastructure and assets. With a proactive approach and expertise in implementation, SMSIU is focused on deploying and maintaining robust security measures to mitigate risks effectively.

One of SMI's primary responsibilities is to provide "Security Implementation & Management" services, aimed at fortifying the organization's defenses against cyber threats. Leveraging advanced technologies and best practices, SMI implements security solutions tailored to organizational specific needs, ensuring optimal protection.

Moreover, SMI operates with a holistic approach, integrating capabilities across people, processes, and technology. Rather than being solely tool-centric, SMI emphasizes the fusion of capabilities to take decisive actions in policy creation and risk mitigation.

In essence, SMI plays a pivotal role in safeguarding the organization's digital assets and operations. By providing proactive security management, robust implementation of security measures, and continuous enhancements, SMI helps mitigate risks, protect business functions, and preserve organizational functionality.

Main Services Under SMSIU

DSU Services	Description
DDoS Mitigation Services	Our DDoS Mitigation Services ensure uninterrupted online operations by swiftly identifying and mitigating DDoS attacks. Using advanced monitoring tools, we detect threats early and deploy mitigation measures promptly to restore normal service. With proactive monitoring and rapid response, we safeguard organizational digital infrastructure from disruptions caused by DDoS L4 and L7 attacks, ensuring continuous availability of online services.
WAF Services	Our WAF Services offer robust protection for web applications, shielding against the top 10 OWASP attacks and any abnormal requests towards web applications.
EDR/XDR	EDR/XDR Services offer comprehensive protection across endpoints and the digital environment. Using advanced threat detection and real-time monitoring by SOC team, we swiftly identify and neutralize threats, ensuring continuous security.
SIEM Services	Our SIEM Services offer centralized monitoring and analysis of security events across organizational digital environment by aggregating and correlating data from various sources.
Preventive DNS	Our Preventive DNS Services provide proactive protection against malicious activities by blocking access to known malicious domains before they can pose a threat. Leveraging advanced DNS filtering technologies, we ensure that users are directed away from potentially harmful websites and domains.

Defensive Security Unit

The Defensive Security Unit (DSU) at STS security department is a dedicated team focused on detecting and preventing malicious activities both within and outside the organization. With advanced detection and response capabilities, DSU ensure efficient responses with minimal or no false positives, with well-defined Service Level Agreements (SLAs) demonstrate a high level of commitment to their objectives.

The primary objective is "Events Monitoring & reporting" Service is to rapidly detect and respond to any malicious activity. This is facilitated by their use of Next-Generation Security Information and Event Management (SIEM) system and proactive threat hunting techniques.

Operating around the clock with vigilant 24x7 service provides robust defense measures built on a secure architecture and advanced technology stack. By leveraging this service, enterprises can not only reduce risks to their business functions but also protect their brand reputation.

The DSU operates cohesively, integrating capabilities across people, processes, and technology. Unlike traditional security operations centers, our approach is not tool-centric but rather focuses on leveraging a fusion of capabilities to take decisive actions and rapidly contain threats.

Main Services Under DSU

DSU Services	Description
Monitoring, Analyzing and Reporting	Entrust our SOC Monitoring, Analyzing, and Reporting services to maintain a vigilant eye on your digital environment 24/7. Our dedicated team leverages advanced tools to detect and analyze threats in real-time, ensuring proactive defense measures.
Incident Handling & Response	Our team provides a strategic approach to incident handling and response. We aim to minimize damage and recovery time by efficiently detecting and managing cyber threats.
Threat Hunting	Proactively hunt for hidden threats in your systems. Our experts use advanced techniques to uncover unseen attackers, minimizing risks before they cause damage. This improves your overall security posture.
Advanced threat hunting Integration	Access a vast library of pre-built Sigma rules for leading SIEM , reduce time spent building detection logic which is allowing quicker identification and mitigation of threats and leverage SOC Prime's tools to hunt for threats across your security data lake.
Malware Analysis	We dissect suspicious files to understand their goals (data theft, disruption, etc.), how they operate, and potential damage. This knowledge helps us stop them and protect your systems.
	collecting and analyzing network traffic and device logs to investigate security incidents.

Network & Log Forensics	This helps identify attack origin, timeline, and impacted data, allowing for informed response and prevention of future attacks.
Phishing Email Analysis	dissecting suspicious emails to identify scams. By examining sender details, content, links, and attachments, we expose these attempts to steal your data or infect devices. This vigilance helps prevent cyberattacks and safeguards your organization.
Dark Web Monitoring	scours hidden corners of the internet for leaks of your data, like passwords or social security numbers, … etc. By tracking these marketplaces, it alerts you to potential threats and helps you take action to protect your company.
Digital Risk Protection	safeguards your online assets and reputation. It proactively hunts threats across the web, including dark marketplaces, to prevent attacks and data breaches before they happen.
DNS Protection	Shields you from online threats. It acts like a security guard, filtering malicious websites and preventing malware infections, this keeps your devices and company safe.
DDOS Protection	Acts like a shield for your online resources, filtering out malicious traffic from a DDoS attack while allowing legitimate users through. This keeps your website or network available during an attack
Threat Research & Analysis	Our team continuously researches and analyzes the latest cyber threats, including emerging malware strains, attacker tactics, techniques, and procedures (TTPs). This in-depth analysis helps us understand attacker motivations and capabilities.
Customized Reporting & Alerts	The DSU Unit tailors reports and alerts to your specific needs and threat landscape. These reports provide actionable insights into the latest threats and vulnerabilities, enabling you to make informed security decisions.