SSI™

Shared Responsibility Model

It takes two to tango

Security and Compliance is a shared responsibility between SSI and the customer.

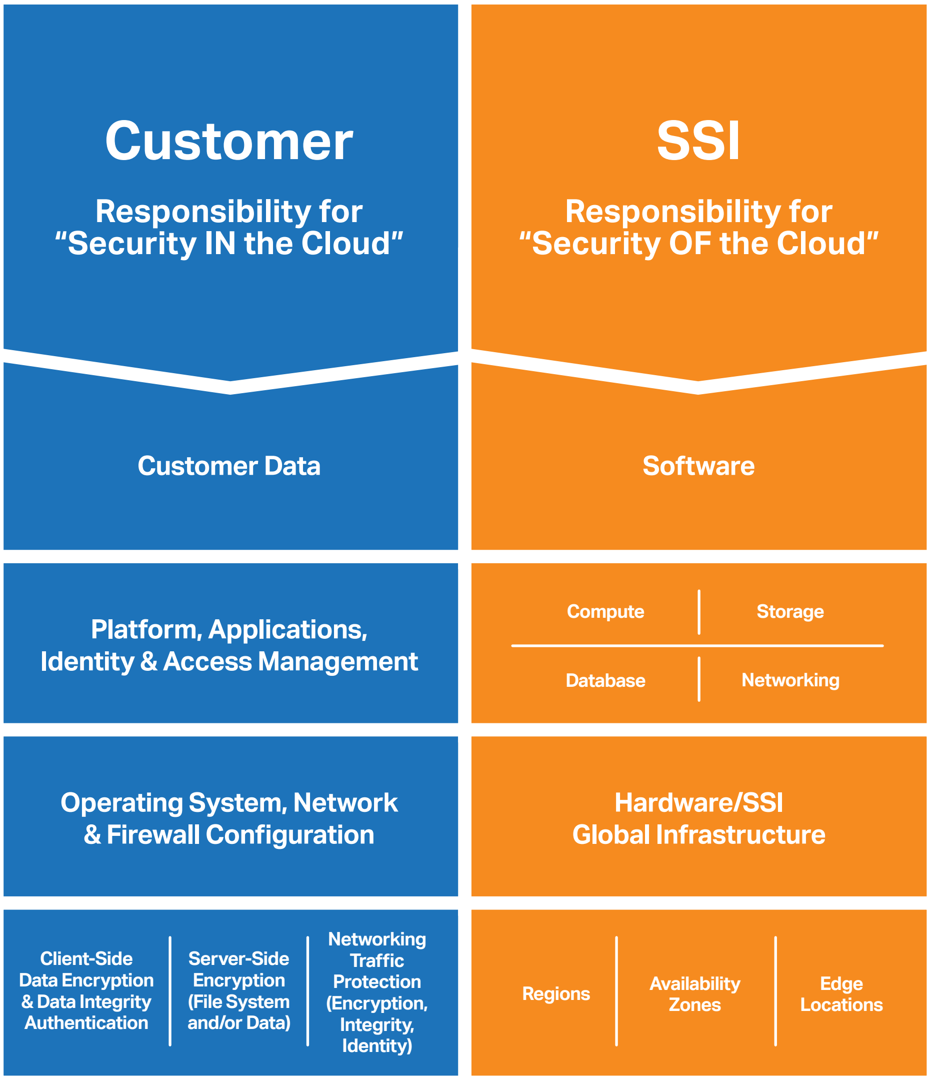
This shared model can help relieve the customer's operational burden as SSI operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Unless covered by server management services, the customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the SSI provided firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment.

SSI RESPONSIBILITY "SECURITY OF THE CLOUD"

SSI is responsible for protecting the infrastructure that runs all of the services offered in the SSI Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run SSI Cloud services.

CUSTOMER RESPONSIBILITY "SECURITY IN THE CLOUD"

Customer responsibility will be determined by the SSI Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, if one of our clients is only paying and consuming Infrastructure as a Service (IaaS) in our datacenter, without any type of server support, clients are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the SSI-provided firewall (called a security group) on each instance. If our clients subscribe to server monitoring and management, SSI will be responsible for the management of the guest operating system (including updates and security patches) and SSI will include NGAV licensing and monitoring on the servers. Unless specifically requested and provided as part of the contract, SSI will not perform any vulnerability management or SOC/SIEM services. Customers are responsible for patching 3rd party software (Non-Windows OS) for vulnerabilities.



Customer

Responsibility for “Security IN the Cloud”

Customer Data

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-Side Data Encryption & Data Integrity Authentication | Server-Side Encryption (File System and/or Data) | Networking Traffic Protection (Encryption, Integrity, Identity)

SSI

Responsibility for “Security OF the Cloud”

Software

Compute | Storage | Database | Networking

Hardware/SSI Global Infrastructure

Regions | Availability Zones | Edge Locations

This customer/SSI shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between SSI and its customers, so is the management, operation and verification of IT controls shared. SSI can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the SSI environment that may previously have been managed by the customer. As every customer is deployed differently in SSI, customers can take advantage of shifting management of certain IT controls to SSI which results in a (new) distributed control environment. Customers can then use the SSI control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

INHERITED CONTROLS

Controls which a customer fully inherits from SSI.

- **Physical and Environmental controls**

SHARED CONTROLS

Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, SSI provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of SSI services. Examples include:

- **Patch Management**
  SSI is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

- **Configuration Management**
  SSI maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

- **Awareness & Training**
  SSI trains SSI employees, but a customer must train their own employees.

CUSTOMER SPECIFIC

Controls which are solely the responsibility of the customer based on the application they are deploying within SSI services. Examples include:

- **Service and Communications Protection or Zone Security** which may require a customer to route or zone data within specific security environments.

SSI™
Managed Technology Solutions.

SSI provides secure, regulatory-compliant managed IT services demanded by compliant-sensitive organizations including those in healthcare, manufacturing, government, non-profit, finance, and education.
By actively investing in our team members, processes, and tools, SSI’s customized IT support services continue to expand. The company provides its clients with a clear path to digital transformation via a broad portfolio of managed IT services, cyber security offerings, and cloud solutions all managed by an expert team.

Learn more by calling 800 774 9935 or visiting ssi-net.com