

ADDENDUM TO SECURITY TECHNOLOGY MANAGEMENT SERVICE DESCRIPTION

Public Cloud Security (IaaS)

Scope, Features and Responsibilities

The Security Technology Management service provides support for public cloud security tools with the following feature sets:

- Service Operations activities and responsibilities described in the Security Technology Management (Cloud) service description.
- Integration to core detection capabilities is provided by the Managed Detection service.

Trustwave provides 24X7 Threat Detection and configuration management for the Client's public cloud, focusing on the following:

- Visibility of public cloud assets and compliance with Client policies
- Enforcing consistent governance and compliance across multi-cloud environments
- Management of public cloud security tool configurations and settings
- Providing remediation recommendations
- Threat detection and investigation across public cloud

RACI Chart

Service features described in the following RACI chart (depending on purchased services):

Table 1: IaaS RACI

		Customer	Trustwave
Implementation and Onboarding	Configure cloud environment permissions to establish connection	RA	CI
	Provision Cloud Security Platform and apply settings (when applicable)	CI	RA
	Confirm resource monitoring and data ingestion.	CI	RA
	Define and enable customized policies, alerts and remediation steps; or enable the out-of-the-box compliance standard and rulesets provided by cloud security platform	CI	RA

	Application of necessary configurations on Client-side services for integration with remediation services	RA	CI
	Integrate into Trustwave Fusion Platform	I	RAC
Ongoing Operations	Generate alerts for resources in policy violation	I	RAC
	Threat Detection and Investigation with remediation recommendations based on established runbook.	CI	RA
	Execute guided or automated remediation.	RA	CI
	Generate compliance, alert, and audit reports.	I	RAC
	Implementation of policy or configuration change requests	CI	RA
	Provide technical assistance limited to general platform support or product related enquiries.	CI	RA
	Maintenance of Client cloud platform and all resources.	RAC	I
	Escalations to solution vendor	CI	RA

R- Responsible, A- Accountable, C- Consulted, I- Informed