Platform: the cloud platform that Thales is providing

CSP (Cloud service provider) : the underlying service and infrastructure on top of which the platform sits. It may be provided by a third party or it may be provided by Thales.

Digital Product: A product which is developped by a customer on top of the platform**.** Usually, there are several digital products per platform.

Platform entity: the Thales entity which provides the platform

	Team who develops/integrates a containers to k8saas	Thales Platform k8saas Team
O.1 Container Management		
O.1.1 Build, Patch, Troubleshoot a container	A / R	
O.1.2 Build & Monitor container application-level metrics & dashboards as per Alerting, Monitoring and Logging Policy	A / R	C
O.1.3 Ensure container application-level, store-level performances, tuning and troubleshooting.	A / R	C
O.1.4 Ensure container application-level log configuration, draining and local house-keeping.	A / R	
O.1.5 Patch and Troubleshoot third-party libraries/containers globally managed by k8saas team	I	A / R
O.2 Kubernetes Storage Management		
O.2.1 Add a custom storage class	I	A/R
O.2.2 Create a persistent volume	A / R	
O.3 Change Management		
O.3.1 Trigger a Change on "Sandbox" kubernetes cluster for a container.	A / R	
O.3.2 Approve a Change on "Sandbox" kubernetes cluster for a container.	A / R	
O.3.3 Trigger a Change on "Production" kubernetes cluster for a container.	A / R	I
O.3.4 Approve a Change on "Production" kubernetes cluster for a container.	A / R	I
O.3.5 Trigger a Minor Change on "Sandbox" environment for a kubernetes cluster		A / R
O.3.6 Trigger a Major Change on "Sandbox" environment for a kubernetes cluster	I	A / R
O.3.7 Trigger a Minor Change on "prod" environment for a kubernetes cluster	I	A / R
O.3.8 Trigger a Major Change on "prod" environment for a kubernetes cluster	C	A / R
O.4 Incident Management		
O.4.1 Initiate/Update/Close an incident for a container	A / R	I
O.4.2Manage an operation incident for a "Sandbox" environment	A / R	I
O.4.3 Manage an operation incident for a "Production" environment	A / R	I
O.4.4 Automatically remediate an operation incident for a "Sandbox" environment as per K8Saas Automated Incident Response Policy.	I	A / R

O.4.5 Automatically remediate an operation incident for a "Production" environment as per K8Saas Automated Incident Response Policy.	I	A / R
O.4.6 Ask for applying a tag-based exception on resources of a container to not benefit from the Thales Platform Provider baseline remediation.	A / R	
O.4.7 Ensure services continuity, training and procedure application for critical containers as per Business Continuity Plan.	A / R	I
O.4.8 Supervise containers as per Alerting, Monitoring and Logging Policy.	A / R	I
O.4.9 Initiate/Update/Close an incident for a cluster (minor incident)	I	A / R
O.4.10 Initiate/Update/Close an incident for a fleet of cluster (major incident)	I	A / R
O.4.11 Supervise kubernetes cluster as per Alerting, Monitoring and Logging Policy.	I	A / R
O.4 Service Request Management		
O.4.1 Initiate/Update/Close a Service Request for a container	R	A
O.4.2 Initiate/Update/Close a Service Request for kubernetes managed services	R	A
O.4.3 Initiate/Update/Close an Cloud Service Provider case (CSP is Consulted)	I	A / R
O.5 Backup Management		
O.5.1 Backup of disks Volume based on k8saas Backup Policy.		A / R
O.5.2 Backup of containers based on k8saas Backup Policy.		A / R
O.5.3 Define all backup policies.		A / R
O.5.4 Request a store or container restoration following k8saas Backup Policy.	A / R	I
O.5.5 Perform restoration activity on a requested store or container.	I	A / R
O.5.6 Monitor backup activity across all k8saas managed services.		A / R
O.6 Infrastructure Scheduling Management		
O.6.1 Create/Update/Delete k8saas Scheduling Policy.		A / R
O.6.2 Ask for a tag-based policy on resources in "Sandbox" or "Prod" environment	A / R	I
O.7 Infrastructure Automation		
O.7.1 Deploy infrastructure as part of the k8saas managed services		A / R
O.7.2 Run capacity planning on the overall infrastructure	C	A / R
O.7.3 Manage NSG rules (blacklist)		A / R

O.7.4 Manage Disk encryption keys		A / R
O.7.5 Manage kaas.thalesdigital.io and k8saas.thalesdigital.io domains		A / R
O.7.6 Ask for peerings between landing zones and k8saas	A / R	
O.7.7 Manage peerings between landing zones and k8saas		A / R
O.8 Service Transition Management (promote Staging => prod)		
O.8.1 Request a cluster on "Sandbox" or "Production" environment	A / R	I
O.8.2 On-board a cluster on "Sandbox" or "Production"environment following Service Transition Policy and Process.	I	A / R
O.9 Repository Management		
O.9.1 Create Digital Product/container code repository	A / R	
O.9.2 Manage centrally and for each stage: "Sandbox", "Production" Helm repositories	A / R	
O.9.3 Manage centrally and for each stage: "Sandbox", "Production Container images	A / R	
O.10 Log Management		
O.10.1 Set log configuration for third-party libraries globally managed by Thales Thales Platform Provider		A / R
O.10.2 Set log configuration for OS-level		A / R
O.10.3 Set log configuration for a container at application-level following the Thales Platform Provider Log policy.	A / R	
O.10.4 Define global log policy per environment "Sandbox" & "Production", applicable to all log ingested		A / R
O.10.5 Define log exclusion filter to perform smart draining	A / R	
O.10.6 Search and Query indexed logs for a k8saas (referenced by its *Application Stack Code*).	A / R	
O.11 Compute Management		
O.11.1 Create, Update, Deprecate, Delete a Golden VM Image	A / R	
O.11.2 Create, Update, Deprecate, Delete a Product VM Image part of a Digital Product.	A / R	
O.11.3 Create, Update, Delete Docker container part of Digital Product.	A / R	
O.11.4 Create, Update, Delete serverless function and related packages part of a Digital Product.	A / R	
O.12 IT Service Management		
O.12.1 Create/Update/Delete Zendesk Service Request Catalog item		A / R
O.12.2 Manage Zendesk role & permissions of users and groups	I	A / R

O.13 Expose application to external network		
O.13.1 Deploy internal or external ingress controllers		A / R
O.12.2 Configure ingress for a given container	A / R	

	Team who develops/integrates a containers to k8saas	Thales Platform k8saas Team
S.1 At Rest Protection		
S.1.1 Select & Manage Cloud Service Provider service encryption for all storages		A/R
S.2 In-Transit Protection		
S.2.1 Ensure communications between containers are encrypted		A/R
S.2.2 Manage mTLS certificates		A/R
S.2.3 Disable the default pod to pod encryptions	A/R	
S.3 Certificate Management		
S.3.1 Manage certificates lifecycle as part of the k8saas service offer - https://doc.kaas.thalesdigital.io/docs/k8saas-public-documentation/Features/tls-certificate.html	I	A/R
S.4 Firewall Configuration		
S.4.1 Ensure the Firewall configuration follows the trustnest ISSP		A/R
S.4.2 Manage the exception		A/R
S.4.3 Ensure that any peered network are correctly filtered		A/R
S.5 Tag Management		
S.5.1 Define naming and tagging convention for containers	A/R	
S.5.2 Define and Follows naming and tagging convention for infrastructure resources		A/R
S.6 Penetration Testing		
S.6.1 Issue a penetration test request on containers.	A/R	I
S.6.2 Authorize penetration testing session for a given kubernetes cluster.	I	A/R
S.6.3 Execute a penetration test for a kubernetes cluster.	I	A/R
S.6.4 Report penetration test results to Platform Entity Security Team and users	A/R	I
S.6.5 Ensure penetration test critical and high findings being corrected for containers .	A/R	I

S.6.6 Issue a penetration test request on a kubernetes clusters.		A/R
S.6.7 Authorize penetration testing session for a Digital Platform.		A/R
S.6.8 Execute a penetration test for a Digital Platform.		A/R
S.6.9 Report penetration test results to Platform Entity Security Team and users	I	A/R
S.6.10 Ensure penetration test critical and high findings being corrected for a Digital Platform.		A/R
S.7 Security Patch Management		
S.7.1 Ensure OS security patch baseline is up to date on kubernetes clusters.	I	A/R
S.7.2 Ensure using latest Images to build Product container Images.	A/R	I
S.7.3 Accept security critical patch and associated risks on all live instances being ensured by Platform Entity.	A/R	R
S.7.4 Ensure security patching on all libraries globally managed by Thales Platform Entity.	I	A/R
S.7.5 Ensure Digital Product & third-party libraries required for Digital Product security patching are up to date.	A/R	R
S.7.6 Ensure security patching of any Docker container part of Digital Product is up to date.	A/R	R
S.8 Forensics		
S.8.1 Collect, Filter and organize logs and evidences related to a security incident.	I	A/R
S.8.2 Run Digital Forensic for a security incident.	R	A/R
S.8.3 Build Digital Forensic report for a security incident.	I	A/R
S.9 Compliance Management		
S.9.1 Define, Control & Enforce Platform Entity Security Policy.	I	A/R
S.9.2 Comply with all Platform Entity Security Policy.	R	A/R
S.9.3 Request a compliance certification for a given cluster (like PCI-DSS).	A/R	C
S.9.4 Mandate auditor for compliance audit.	A/R	C
S.9.5 Archive security infrastructure logs (DNS, IAM, Kubernetes master) aligned with Platform Entity Compliance Log Policy.		A/R
S.9.6 Create, Update, Delete assets inventory.		A/R
S.10 Hardening		

S.10.1 Use standard CIS hardening for all containers images.	A/R	
S.10.3 Control CIS hardening is applied on all live instances part of *k8saas.*	I	A/R
S.11 Access Management		
S.11.1 Manage & Operate Egress proxy.	I	A/R
S.11.2 Manage & Operate Ingress proxy	A/R	I
S.11.3 Ensure the ingress configuration follows the trustnest PSSI.		A/R
S.12 Vulnerability Management		
S.12.1 Execute vulnerability network scan and report findings for k8saas	I	A/R
S.12.2 Execute application vulnerability scan and report findings for containers	A / R	I
S.12.3 Correct "Critical" and "High" OS vulnerability following the trustnest SLA for k8saas	I	A/R
S.12.4 Correct "Critical" and "High" OS vulnerability following the trustnest SLA for containers	A/R	I
S.13 kuberntes cluster Management		
S.13.1 Request to create or to delete *k8saas cluster*	A/R	C
S.13.2 Create, Update, Delete k8saas cluster	I	A/R
S.14 Network Management		
S.14.1 Create, Update, Delete Route tables	I	A/R
S.14.2 Create, Update, Delete Peering	I	A/R
S.15 Connectivity Management		
S.15.1 Expose an application to external network	A/R	
S.15.2 Ask for a Zscaler VPN account	A/R	I
S.15.3 Troubleshoot VPN issue (aws VPN/ zscaler)	A/R	C
S.15.4 Manage the trustnest blacklisting ips		A/R
S.15.5 Ask for a custom interconnection	A/R	C
S.15.6 Manage the custom interconnection	I	A/R
S.15.7 Use WAF for all application exposed on external network	A/R	
S.15.8 Discard a WAF rule	A/R	C

S.16 Account Management		
S.16.1 Ask for a CSP Account creation	A/R	I
S.16.4 Ask for a Service Account creation	A/R	I
S.17 User Management		
S.17.1 Ask for a new role (dev, devops, viewer, level1, admin	A/R	I
S.17.2 Manage roles	I	A/R
S.18 Security Incident Management		
S.18.1 Notify security incident for a Digital Product supporting infrastructure	I	A/R
S.18.2 Analyze security incident for a Digital Product supporting infrastructure	R	A/R
S.18.3 Respond to security incident for a Digital Product supporting infrastructure	R	A/R
S.18.4 Escalate security incident for a Digital Product supporting infrastructure		A/R
S.18.5 Report security incident for a Digital Product supporting infrastructure	I	A/R
S.18.6 Create, Update, Delete Security Incident Response Procedure for a Digital Product supporting infrastructure	I	A/R