RA-1, RI-1 and RC-1 Traceability and Gap Analysis

This page will serve as a placeholder to get the matrix complete in collaboration between CNTT and OPNFV (until interested parties are satisfied). To "publish", set of pull requests will be issued in GitHub (RA-1). This page when then be deleted.

RM Requirements (TBD)

Infrastructure Profiles Catalog ()

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	RM 4.2.1.1 RM 4.2.4	Predefined Flavors	Catalog of Predefined Flavor Geometries	RA-1 "4.2.2.5. Compute Nodes"	3.2 VNF Category	Yes	Armada Charts	Please see the manifests	Functional		
2	RM 4.2.2	Flavor Networking	Network Interface Specifications	RA-1 "4.2.2.9 Compute node configurations for Profiles and Flavors"	3.2 VNF Category	Yes	Armada Charts		Functional		
3	RM 4.2.3	Flavor Storage Extensions	Flavor Storage Extensions	RA-1 "4.4.1. Support for Profiles and T-shirt instance types"	3.2 VNF Category	Yes	Armada Charts		Functional		
4	RM 4.2.5 Also RM 5.2.1	Profile Capabilities	Profile Capabilities includes specifications for capabilities such as CPU Pinning, NUMA support, SR-IOV, FPGA, etc.	RA-1 "4.4.1. Support for Profiles and T-shirt instance types"	3.3 NFVI SW Profile	Yes	Armada Charts		Functional		
5	RM 5.2.3	Virtual (Overlay) Networking	Virtual (Overlay) Networking including vNIC interfaces, Protocols (VXLAN, Geneve, ...), NAT, Security Groups, HW Offload, crypto acceleration	RA-1 "4.2.3. Network Fabric"	3.3 NFVI SW Profile	Yes	Armada Charts		Functional		
6	RM 5.4	HW Profiles	Hardware Profiles including configurations for compute, storage, networking, PCIe	RA-1 "4.2.2. Compute"	3.4 NFVI HW Profile	Yes	Armada Charts		Functional		

RA-1 Requirements (required)

Note: RI-1 incorporates all RA-1 Requirements by reference in RI-1 2.2 Reference Architecture Requirement. The ***provisioning and deployment of the Platform*** is covered in RI-1 8.5.1.1 which links to Airship manifests configuration documentation. Hence, there is no RI-1 Traceability column in the following tables.

General Requirements (RA-1 Section 2.3.1)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.gen.ost.01	Open source	The Architecture **must** use OpenStack APIs.	RA-1 5.3. Consolidated Set of APIs	Yes	Armada Chart	Manifests with Airship 2.0 will replace with helm operator	Functional		
2	req.gen.ost.02	Open source	The Architecture **must** support dynamic request and configuration of virtual resources (compute, network, storage) through OpenStack APIs.	RA-1 5.3. Consolidated Set of APIs	Yes	NA	Once OpenStack installed this is intrinsic capability	Functional		

3	req.gen.rsl.01	Resiliency	The Architecture **must** support resilient OpenStack components that are required for the continued availability of running workloads.	RA-1 3.3.1. VIM Core services	Yes	NA	Once k8s installed this is intrinsic capability	OSTK components resiliency	missing Al Morton There are several HA tests conducted as part of OVP 1.0, are they sufficient? Yardstick TC025 and/or TC045	supported through redundancy; redundancy and recoverability can be managed through k8s
4	req.gen.avl.01	Availability	The Architecture **must** provide High Availability for OpenStack components.	RA-1 4.2 Underlying Resources	Yes	NA	Once k8s installed this is intrinsic capability	OSTK Components High Availability	missing Al Morton There are several HA tests conducted as part of OVP 1.0, are they sufficient?	supported through redundancy; redundancy and recoverability can be managed through k8s

Infrastructure Requirements (RA-1 Section 2.3.2)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.inf.com.01	Compute	The Architecture **must** provide compute resources for VM instances.	RA-1 3.3.1.4 "Cloud Workload Services"	Yes	Armada Chart		Functional	Functest	
2	req.inf.com.04	Compute	The Architecture **must** be able to support multiple CPU SKU options to support various infrastructure profiles (Base, and Network Intensive).	RA-1 4.4.1. "Support for Profiles and T-shirt instance types"	Yes	Armada Chart	Post processing	Functional	missing	needs to be confirmed (same as RM requirements)
3	req.inf.com.05	Compute	The Architecture **must** support Hardware Platforms with NUMA capabilities.	RA-1 4.4.1. "Support for Profiles and T-shirt instance types"	Yes	Armada Chart		Functional	Functest	Functest supports tuning a few inputs such flavor extra specs (e.g. hugepages). All tests can be executed multiple times (basic then network intensive) comment acknowledged, no action required

4	req.inf.com.06	Compute	The Architecture **must** support CPU Pinning of the vCPUs of VM instance.	RA-1 4.4.1. "Support for Profiles and T-shirt instance types"	Yes	Armada Chart		Functional	Functest	Functest supports tuning a few inputs such flavor extra specs (e.g. hugepages). All tests can be executed multiple times (basic then network intensive) comment acknowledged, no action required
5	req.inf.com.07	Compute	The Architecture **must** support different hardware configurations to support various infrastructure profiles (Base, and Network Intensive).	RA-1 3.3.3. "Host aggregates providing resource pooling"	Yes	Armada chart		Functional	Functest	Functest supports tuning a few inputs such flavor extra specs (e.g. hugepages). All tests can be executed multiple times (basic then network intensive) comment acknowledged, no action required
6	req.inf.com.08	Compute	The Architecture **must** support allocating certain number of host cores /threads to non-tenant workloads such as for OpenStack services.	Dedicating host core /sibling threads to certain workloads (e.g., OpenStack services. Please see example, "Configuring libvirt compute nodes for CPU pinning"	Yes	Armada chart		Functional		
7	req.inf.com.09	Compute	The Architecture **must** ensure that the host cores/threads assigned to a workload are thread-sibling aware: that is, that a core and its associated SMT threads are either all assigned to non-tenant workloads or all assigned to tenant workloads.	Achieved through configuring the "cpu_dedicated_set" and "cpu_shared_set" parameters in nova.conf correctly.	Yes	Armada chart		Functional		Al Morton Possibly verified with VSPERF testing (Cross-NUMA Test Results). Also ETSI NFV TST009, clause 12.4 and Annex D.

8	`req.inf.stg.01`	Storage	The Architecture **must** provide remote (not directly attached to the host) Block storage for VM Instances.	RA-1 3.4.2.3. "Storage"	Yes	Armada chart		Functional	Functest	too generic and should mention the ref to the mandatory capabilities and the status expected. 130 single tests about volumes amongst tempest_cinder, tempest_full, tempest_scenario and tempest_slow (+indirect testing in case of tempest_heat) addressed in req.int.api.03 below (PR #1622 merged)
9	`req.inf.stg.02`	Storage	The Architecture **must** provide Object storage for VM Instances. Operators **may** choose not to implement Object Storage but must be cognizant of the risk of "Compliant VNFs" failing in their environment.	OpenStack Swift Service (RA-1 4.3.1.4 "Swift")	Yes	Armada chart		Functional	Functest	too generic and should mention the ref to the mandatory capabilities and the status expected. 140 single tests about object storage amongst tempest_full, tempest_scenario and tempest_slow (+indirect testing in case of tempest_heat) addressed in req.int.api.04 below (PR #1622 merged)

10	req.inf.stg.03 move to Recommendations	Storage	The Architecture **may** provide a file system service (file system storage solution) for VM Instances.	RA-1 4.2.4. "Storage Backend"	Yes	Armada chart		Functional	Out of CNTT RC (may) + an API proposing this feature should be proposed in CNTT first	The tempest plugin could be added in Functest if it makes sens (IaaS verification). Useless on CNTT side right now **Bug here!**
11	req.inf.stg.04 move to Recommendations	Storage	The Architecture **may** support Software Defined Storage (SDS) that seamlessly supports shared block storage, object storage and flat files.	RA-1 4.2.4.1. "Ceph Storage Cluster"	Yes	Armada chart		Functional	Out of CNTT RC (may)	As far as I understand It's out of CNTT (implementation design) Ceph is tested thought the mandatory service API by Functest
12	req.inf.stg.06 move to Recommendations	Storage	The Architecture **should** make the immutable images available via location independent means.	RA-1 4.3.1.2. "Glance"	Yes	Armada chart		Functional	Functest	**It's a must requirement according RA1 Chapter5** **Bug here !** Glance is required but not necessarily immutable images – some operators make changes to install needed tools such anti-virus etc.

13	req.inf.stg.07 move to Recommendations	Storage	The Architecture **should** provide high-performance and horizontally scalable VM storage.	RA-1 4.2.4.1. "Ceph Storage Cluster"	Yes	Armada chart		Functional	Functest	As far as I understand It's out of CNTT (implementation design) and the related API is a must requirement. Does it make sens to cover ceph from a functional pov (why not benchmarking)? **Bug here!** ceph is not required – during requirement creation there was opposition
14	req.inf.stg.10 ~~duplicate-and-wrong—modify~~ this reqt is for local, req.inf.stg.01 was for "remote" move to Recommendations	Storage	The Architecture **should** provide local Block storage for VM Instances.	RA-1 "Virtual Storage"	Yes	Armada chart		Functional	Functest	
15	req.inf.stg.11 ~~duplicate-and-wrong—modify~~ move to Recommendations	Storage	The Architecture **should** support the Block storage capabilities specified in https://docs.openstack.org/api-ref/block-storage/.	RA-1 5.2.3. "Cinder"	No	NA	Cinder is the Block storage Service	Functional	Functest	**It's a must requirement according RA1 Chapter5** **Bug here !** The original reuirement is to support all Cinder capabilities listed in the refererred to document – and that is not rquired only some features are required

16	req.inf.ntw.01	Network	The Architecture **must** provide virtual network interfaces to VM instances.	RA-1 5.2.5. "Neutron"	No	NA	Neutron	Functional	Functest	
17	req.inf.ntw.02	Network	The Architecture **must** include capabilities for integrating SDN controllers to support provisioning of network services, from the OpenStack Neutron service, such as networking of VTEPs to the Border Edge based VRFs.	RA-1 3.2.5. "Virtual Networking – 3rd party SDN solution"	Yes			Functional	Functest	
18	req.inf.ntw.03	Network	The Architecture **must** support low latency and high throughput traffic needs.	RA-1 4.2.3. "Network Fabric"	No	NA		low latency, high throughput	missing VSPERF BM Tests: p2p and pvp Cloud tests possible with PROX and NFVBench	Al Morton updated: Tests Desc: ETSI NFV TST009, clauses 8 and 9 Note: RA-1 reference is "content to be developed".
19	req.inf.ntw.05	Network	The Architecture **must** allow for East /West tenant traffic within the cloud (via tunnelled encapsulation overlay such as VXLAN or Geneve).	RA-1 4.2.3. "Network Fabric"	Yes			Functional	Functest	
20	req.inf.ntw.07	Network	The Architecture **must** support network resiliency.	RA-1 3.4.2.2. "Network"	No	NA	may be achieved through redundancy	network resiliency	missing	may be achieved through redundancy Al Morton Need the Leaf-Spine switch configurations (not typically confifured in OPNFV Pods).
21	req.inf.ntw.10	Network	The Cloud Infrastructure Network Fabric **must** be capable of enabling highly available (Five 9's or better) Cloud Infrastructure.	RA-1 3.4.2.2. "Network"	No	NA	may be achieved through redundancy	network availability	missing	may be achieved through redundancy Al Morton 5-9's **Not Testable in reasonable time frames. 5 Nines = 53 minutes downtime PER YEAR, average**

22	req.inf.ntw.15	Network	The Architecture **must** support multiple networking options for Cloud Infrastructure to support various infrastructure profiles (Basic Network Intensive).	RA-1 4.2.3.4. "Neutron ML2-plugin Integration" and "OpenStack Neutron Plugins"	Yes	Armada chart		Functional	Functest	As far as I understand It's out of CNTT (implementation design). RA1 Chapter5 sets as mandatory the networking capabilities (already verified by neutron agents and OVN) This requirement is about the support of network options such as SDN through the use of plugins. req.int.api.05 below (PR #1622 merged) deals with your comment about mandatory capabilities
23	req.inf.ntw.16	Network	The Architecture **must** support dual stack IPv4 and IPv6 for tenant networks and workloads.		No	NA		Functional	Functest	
24	req.inf.ntw.17 move to Recommendations	Network	The Architecture **should** use dual stack IPv4 and IPv6 for Cloud Infrastructure internal networks.		Yes			Functional	Functest	Must be clarified. Endpoints are registered by IPv4 or IPv6. **Bug ?** THis is not about APIs but the use of dual stack in Controller nodes

25	req.inf.ntw.18	Network	The Architecture **should** support the network extensions specified in https://docs.openstack.org/api-ref/network/v2/.	RA-1 5.2.5. "Neutron"		Armada chart		Functional		**It's a must requirement according RA1 Chapter5** **Bug here !** Not all network extensions are mandatory – the mandatory are now covered under req.int.api.05
26	req.inf.acc.01 move to Recommendations keep for Baraque	Acceleration	The Architecture **should** support Application Specific Acceleration (exposed to VNFs).	RA-1 3.2.6. "Acceleration" and RA-1 4.3.1.10. "Cyborg"		Armada chart		Functional		Out of CNTT RC (should) + an API proposing this feature should be proposed in CNTT RA1 first
27	req.inf.acc.02 move to Recommendations keep for Baraque	Acceleration	The Architecture **should** support Cloud Infrastructure Acceleration (such as SmartNICs).	"OpenStack Future - Specs defined"		Armada chart		Functional		Out of CNTT RC (should) + an API proposing this feature should be proposed in CNTT RA1 first

VIM Requirements (RA-1 Section 2.3.3)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.vim.01	General	The Architecture **must** allow infrastructure resource sharing.	RA-1 3.2. "Consumable Infrastructure Resources and Services"	No	NA	OpenStack intrinsic	Functional	Functest	
2	req.vim.02 move to Recommendations	General	The Architecture **should** support deployment of OpenStack components in containers.	RA-1 4.3.2. "Containerised OpenStack Services"	Yes	Armada Chart		Functional	Functest	
3	req.vim.03	General	The Architecture **must** allow VIM to discover and manage Cloud Infrastructure resources.	RA-1 5.2.7. "Placement"	No	NA	OpenStack and IPMI	Functional	Functest	
4	req.vim.05	General	The Architecture **must** include image repository management.	RA-1 4.3.1.2. "Glance"	No	NA	Image Service (Glance) (installed as part of OpenStack core services)	Functional	Functest	
5	req.vim.07	General	The Architecture **must** support multi-tenancy.	RA-1 3.2.1. "Multi-Tenancy"	No	NA	OpenStack intrinsic	Functional	Functest	
6	req.vim.08	General	The Architecture **must** support resource tagging.	"OpenStack Resource Tags"	No	NA	OpenStack resource metadata, neutron plugin	Functional	Functest	

Interfaces & API Requirements (RA-1 Section 2.3.4)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.int.api.01	API	The Architecture **must** provide APIs to access to the authentication service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.1 "Keystone"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
2	req.int.api.02	API	The Architecture **must** provide APIs to access to the image management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.2 "Glance"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
3	req.int.api.03	API	The Architecture **must** provide APIs to access to the block storage management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.3 "Cinder"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
4	req.int.api.04	API	The Architecture **must** provide APIs to access to the object storage management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.4 "Swift"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
5	req.int.api.05	API	The Architecture **must** provide APIs to access to the network management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.5 "Neutron"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
6	req.int.api.06	API	The Architecture **must** provide APIs to access to the compute resources management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.6 "Nova"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
7	req.int.api.07	API	The Architecture **must** provide GUI access to tenant facing cloud platform core services.	RA-1 4.3.1.9 "Horizon"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
8	req.int.api.08	API	The Architecture **must** provide APIs needed to discover and manage Cloud Infrastructure resources.	RA-1 5.2.7. "Placement"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
9	req.int.api.09	API	The Architecture **must** provide APIs to access to the orchestration service.	RA-1 5.2.8 "Heat"	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	

10	req.int.api.10	API	The Architecture must expose the latest version and microversion of the APIs for the given CNTT OpenStack release for each of the OpenStack core services.	RA-1 5.2 Core OpenStack Services APIs	No	NA	OpenStack APIs for deployment manifests should include the details	Functional	Functest	
11	req.int.acc.01 move to Recommendations	Acceleration	The Architecture **should** provide an open and standard acceleration interface to VNFs.	RA-1 2.3.4. (was RA-1 5.3.4 - "Cyborg")	No	NA	Acceleration Service (Cyborg) for deployment manifests should include the details	Functional	Functest	

Tenant Requirements (RA-1 Section 2.3.5)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.tnt.gen.01	General	The Architecture **must** support multi-tenancy.	**duplicate of req.vim.07**		NA				
2	req.tnt.gen.02	General	The Architecture **must** support self-service dashboard (GUI) and APIs for users to deploy, configure and manage their workloads.	RA-1 4.3.1.9 "Horizon" and 3.3.1.4 Cloud Workload Services	No	NA	Horizon (installed as part of OpenStack core services)	Functional	Functest	

Operations & LCM Requirements (RA-1 Section 2.3.6)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.lcm.gen.01	General	The Architecture **must** support zero downtime expansion/change of physical capacity (compute hosts, storage increase/replacement).		Yes	Armada Chart		infra expansion	missing	
2	req.lcm.adp.02	Automated deployment	The Architecture **must** support hitless upgrades of software provided by the cloud provider so that the availability of running workloads is not impacted.		Yes	Armada Chart	internally will trigger k8s	software upgardes	missing (Airship?)	

Assurance Requirements (RA-1 Section 2.3.7)

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.asr.mon.01	Integration	The Architecture **must** include integration with various infrastructure components to support collection of telemetry for assurance monitoring and network intelligence.		Yes	Armada chart	Prometheus & Grafana	Functional	Functest	
2	req.asr.mon.03	Monitoring	The Architecture **must** allow for the collection and dissemination of performance and fault information.		Yes	Armada chart	CollectD	performance /fault data	missing	Al Morton Barometer makes this info available, and VSPERF can collect telemetry while testing.

3	req.asr.mon.04	Network	The Cloud Infrastructure Network Fabric and Network Operating System **must** provide network operational visibility through alarming and streaming telemetry services for operational management, engineering planning, troubleshooting, and network performance optimisation.		No	NA	needs LMA platform installed	telemetry	missing - alarming and reporting on barometer via prometheus already available via barometer work. Requirements not clear to find out whats needed of physical network	

Security Requirements (RA-1 Section 2.3.8) | Needs to be updated with latest Security Requirements – DONE

	Ref#	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	req.sec.gen.01	General	The Architecture **must** provide tenant isolation.		No	NA	OpenStack intrinsic	Functional	Functest	
2	req.sec.gen.02	General	The Architecture **must** support policy based RBAC.	**6.3.1.4 RBAC**	Yes	Armada Chart		Functional	Functest	
3	req.sec.gen.03	General	The Architecture **must** support a centralised authentication and authorisation mechanism.	6.3.1.2 Authentication and 6.3.1.3 Authorization	No	NA	Keystone (installed as part of OpenStack core services)	Functional	Functest	
4	req.sec.zon.01	Zoning	The Architecture **must** support identity management (specific roles and permissions assigned to a domain or tenant).	6.3.1.1 Identity	No	NA	Keystone (installed as part of OpenStack core services)	Functional	Functest	
5	req.sec.zon.02	Zoning	The Architecture **must** support password encryption.		No	NA	Barbican (installed as part of OpenStack core services)	Functional	Functest	
6	req.sec.zon.03	Zoning	The Architecture **must** support data, at-rest and in-flight, encryption.	6.3.3 Confidentiality and Integrity	Yes		TLS 1.2+ (in-flight) at-rest use ceph default encryption	Functional	missing	
7	req.sec.zon.04	Zoning	The Architecture **must** support integration with Corporate Identity Management systems.		Yes	Armada chart		integration	missing	
8	req.sec.cmp.02	Compliance	The Architecture **must** comply with all applicable standards and regulations.		No	NA		security standards	missing in Functest. Captured in Telco TCs Security	
9	req.sec.cmp.03	Compliance	The Architecture **must** comply with all applicable regional standards and regulations.		No	NA		security standards	missing	
10	req.sec.ntw.03	Networking	The Architecture **must** have the underlay network incorporate encrypted and/or private communications channels to ensure its security.	6.3.3.3 Confidentiality and Integrity of tenants Data	No	NA		Functional	missing	
11	req.sec.ntw.04	Networking	The Architecture **must** configure all of the underlay network components to ensure the complete separation from the overlay customer deployments.	4.2.3.2 High Level Logical Network Layout	No	NA		network isolation	missing	
12	req.sec.ntw.05	Networking	The Architecture **must** have the underlay network include strong access controls that adhere to the V1.1 NIST Cybersecurity Framework.	6.3.1 Platform Access	No	NA		network access control	missing	

System Hardening (RA-1 Section 2.3.8.1)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec. gen.001	Hardening	The Platform **must** maintain the state to what it is specified to be and does not change unless through change management process.	7.2.2. Configuration Management	Yes	Armada chart	Armada chart pushes the config to fix security	security hardening		
2	sec. gen.002	Hardening	All systems part of Cloud Infrastructure **must** support password hardening (strength and rules for updates (process), storage and transmission, etc.)		Yes			security hardening		
3	sec. gen.003	Hardening	All servers part of Cloud Infrastructure **must** support a root of trust and secure boot	6.3.6 Security LCM	Yes			security hardening		
4	sec. gen.004	Hardening	The Operating Systems of all the servers part of Cloud Infrastructure **must** be hardened	6.3.2 System Hardening	Yes			security hardening		
5	sec. gen.005	Hardening	The Platform **must** support Operating System level access control	6.3.1 Platform Access	Yes			security hardening		
6	sec. gen.006	Hardening	The Platform **must** support Secure logging	6.3.7 Security Audit Logging	Yes			security hardening		
7	sec. gen.007	Hardening	All servers part of Cloud Infrastructure **must** be Time synchronized with authenticated Time service		Yes	Armada chart		security hardening		
8	sec. gen.008	Hardening	All servers part of Cloud Infrastructure **must** be regularly updated to address security vulnerabilities	6.3.2 System Hardening	Yes			security hardening		
9	sec. gen.009	Hardening	The Platform **must** support Software integrity protection and verification	6.3.3 Confidentiality and Integrity	No			security hardening		
10	sec. gen.010	Hardening	The Cloud Infrastructure **must** support Secure storage (all types)	6.3.6 Security LCM	Yes			security hardening		
11	sec. gen.012	Hardening	The Operator **must** ensure that only authorized actors have physical access to the underlying infrastructure.		Yes			security hardening		
12	sec. gen.013	Hardening	The Platform **must** ensure that only authorized actors have logical access to the underlying infrastructure.	6.3.1 Platform Access	Yes			security hardening		

Platform and Access (RA-1 Section 2.3.8.2)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec. sys.001	Access	The Platform **must** support authenticated and secure APIs, API endpoints. The Platform **must** implement authenticated and secure access to GUI	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
2	sec. sys.002	Access	The Platform **must** support Traffic Filtering for workloads (for example, Fire Wall)	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
3	sec. sys.003	Access	The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
4	sec. sys.004	Access	The Cloud Infrastructure **must** support Secure network channels	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
5	sec. sys.005	Access	The Cloud Infrastructure **must** segregate the underlay and overlay networks	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		

6	sec. sys.006	Access	The Cloud Infrastructure **must** be able to utilize the Cloud Infrastructure Manager identity management capabilities	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	No		Keystone (installed as part of OpenStack core services)	security access		
7	sec. sys.007	Access	The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control)	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			Functional	Functest	RBAC
8	sec. sys.008	Access	The Platform **must** be able to assign the Entities that comprise the tenant networks to different trust domains. (Communication between different trust domains is not allowed, by default.)	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
9	sec. sys.009	Access	The Platform **must** support creation of Trust Relationships between trust domains. These maybe uni-directional relationships where the trusting domain trusts another domain (the “trusted domain”) to authenticate users for them or to allow access to its resources from the trusted domain. In a bidirectional relationship both domain are “trusting” and “trusted”.	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	Yes			security access		
10	sec. sys.010	Access	For two or more domains without existing trust relationships, the Platform **must not** allow the effect of an attack on one domain to impact the other domains either directly or indirectly	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	No			security access		
11	sec. sys.011	Access	The Platform **must not** reuse the same authentication key-pair (for example, on different hosts, for different services)	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	No			security access		
12	sec. sys.012	Access	The Platform **must** only use secrets encrypted using strong encryption techniques, and stored externally from the component (e.g., Barbican (OpenStack))	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	No		Barbican (installed as part of OpenStack core services)	security access		
13	sec. sys.013	Access	The Platform **must** provide secrets dynamically as and when needed	[6.3.1 Platform Access](https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md#631-platform-access)	No		Barbican (installed as part of OpenStack core services)	security access		

Confidentiality and Integrity (RA-1 Section 2.3.8.3)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec.ci. 001	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of data at rest and in-transit	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No		Keystone (installed as part of OpenStack core services)	security confidentiality & integrity		
2	sec.ci. 003	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of data related metadata	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No			security confidentiality & integrity		
3	sec.ci. 004	Confidentiality	The Platform **must** support Confidentiality of processes and restrict information sharing with only the process owner (e.g., tenant).	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No			Functional	Functest	Tenant isolation

4	sec.ci.005	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of process-related metadata and restrict information sharing with only the process owner (e.g., tenant).	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No			security confidentiality & integrity		
5	sec.ci.006	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of workload resource utilization (RAM, CPU, Storage, Network I/O, cache, hardware offload) and restrict information sharing with only the workload owner (e.g., tenant).	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No			security confidentiality & integrity		
6	sec.ci.007	Confidentiality/Integrity	The Platform **must not** allow Memory Inspection by any actor other than the authorized actors for the Entity to which Memory is assigned (e.g., tenants owning the workload), for Lawful Inspection, and by secure monitoring services. Admin access must be carefully regulated	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No			security confidentiality & integrity		
7	sec.ci.008	Confidentiality	The Cloud Infrastructure **must** support tenant networks segregation	[6.3.3 Confidentiality and Integrity](./chapter06.md#633-confidentiality-and-integrity)	No		OpenStack inherent capability	Functional	Functest	Tenant isolation

Workload Security (RA-1 Section 2.3.8.4)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec.wl.001	Workload	The Platform **must** support Workload placement policy	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No		Nova /placement	security workload		
2	sec.wl.002	Workload	The Platform **must** support operational security	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No			security workload		
3	sec.wl.003	Workload	The Platform **must** support secure provisioning of workloads	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No			security workload		
4	sec.wl.004	Workload	The Platform **must** support Location assertion (for mandated in-country or location requirements)	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No			security workload		
5	sec.wl.005	Workload	Production workloads **must** be separated from non-production workloads	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No			security workload		
6	sec.wl.006	Workload	Workloads **must** be separable by their categorisation (for example, payment card information, healthcare, etc.)	[6.3.4 Workload Security](./chapter06.md#634-workload-security)	No			security workload		

Image Security (RA-1 Section 2.3.8.5)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec.img.001	Image	Images from untrusted sources **must not** be used	6.3.5 Image Security	No			security image		
2	sec.img.002	Image	Images **must** be maintained to be free from known vulnerabilities	6.3.5 Image Security	No		Internal image scanning tool	security workload		
3	sec.img.003	Image	Images **must not** be configured to run with privileges higher than the privileges of the actor authorized to run them	6.3.5 Image Security	No			security workload		
4	sec.img.004	Image	Images **must** only be accessible to authorized actors	6.3.5 Image Security	No			security workload		
5	sec.img.005	Image	Image Registries **must** only be accessible to authorized actors	6.3.5 Image Security	No			security workload		
6	sec.img.006	Image	Image Registries **must** only be accessible over secure networks	6.3.5 Image Security	Yes			security workload		
7	sec.img.007	Image	Image registries **must** be clear of vulnerable and stale (out of date) versions	6.3.5 Image Security	No			security workload		

Security LCM (RA-1 Section 2.3.8.6)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec. lcm.001	LCM	The Platform **must** support Secure Provisioning, Maintaining availability, Deprovisioning (secure Clean-Up) of workload resources; Secure clean-up: tear-down, defending against virus or other attacks, or observing of cryptographic or user service data	(7.2.2. Configuration Management)	Yes			security LCM		
2	sec. lcm.002	LCM	Operational **must** use management protocols limiting security risk such as SNMPv3, SSH v2, ICMP, NTP, syslog and TLS	(7.2.2. Configuration Management)	Yes			security LCM		
3	sec. lcm.003	LCM	The Cloud Operator **must** implement change management for Cloud Infrastructure, Cloud Infrastructure Manager and other components of the cloud; Platform change control on hardware	(7.2.2. Configuration Management)	No			security LCM		
4	sec. lcm.005	LCM	Platform **must** provide logs and these logs must be regularly scanned	6.3.7 Security Audit Logging	Yes			security LCM		
5	sec. lcm.006	LCM	The Platform **must** verify the integrity of all Resource management requests	6.3.7 Security Audit Logging	No			security LCM		
6	sec. lcm.007	LCM	The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with current time information	(7.2.2. Configuration Management)	No			security LCM		
7	sec. lcm.008	LCM	The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information.	(7.2.2. Configuration Management)	No			security LCM		
8	sec. lcm.009	LCM	The Platform **must** be able to update the tag of newly instantiated, suspended, hibernated, migrated and restarted images with relevant geolocation (geographical) information	(7.2.2. Configuration Management)	No			security LCM		
9	sec. lcm.010	LCM	The Platform **must** log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing).	(7.2.2. Configuration Management)	No			security LCM		
10	sec. lcm.011	LCM	The Platform **must** implement Security life cycle management processes including proactively update and patch all deployed Cloud Infrastructure software.	(7.2.2. Configuration Management)	No			security LCM		

Monitoring and Security Audit (RA-1 Section 2.3.8.7)

The Platform is assumed to provide configurable alerting and notification capability and the operator is assumed to have automated systems, policies and procedures to act on alerts and notifications in a timely fashion. In the following the monitoring and logging capabilities can trigger alerts and notifications for appropriate action.

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec. mon. 001	Monitoring /Audit	Platform **must** provide logs and these logs must be regularly scanned for events of interest	7.4.1. Logging	Yes					
2	sec. mon. 002	Monitoring	Security logs **must** be time synchronised	6.3.7 Security Audit Logging and 7.4.1. Logging	Yes					
3	sec. mon. 003	Monitoring	The Platform **must** log all changes to time server source, time, date and time zones	7.4.1. Logging	Yes					
4	sec. mon. 004	Audit	The Platform **must** secure and protect Audit logs (contain sensitive information) both in-transit and at rest	6.3.7 Security Audit Logging and 7.4.1. Logging	Yes					
5	sec. mon. 005	Monitoring /Audit	The Platform **must** Monitor and Audit various behaviours of connection and login attempts to detect access attacks and potential access attempts and take corrective actions accordingly	7.4. Logging, Monitoring and Analytics (includes Alerting)	No					
6	sec. mon. 006	Monitoring /Audit	The Platform **must** Monitor and Audit operations by authorized account access after login to detect malicious operational activity and take corrective actions accordingly	7.4. Logging, Monitoring and Analytics (includes Alerting)	No					
7	sec. mon. 007	Monitoring /Audit	The Platform **must** Monitor and Audit security parameter configurations for compliance with defined security policies	7.2.2. Configuration Management	No					
8	sec. mon. 008	Monitoring /Audit	The Platform **must** Monitor and Audit externally exposed interfaces for illegal access (attacks) and take corrective security hardening measures	7.4. Logging, Monitoring and Analytics (includes Alerting)	No					
9	sec. mon. 009	Monitoring /Audit	The Platform **must** Monitor and Audit service handling for various attacks (malformed messages, signalling flooding and replaying, etc.) and take corrective actions accordingly	7.4. Logging, Monitoring and Analytics (includes Alerting) - partial	No					

10	sec. mon. 010	Monitoring /Audit	The Platform **must** Monitor and Audit running processes to detect unexpected or unauthorized processes and take corrective actions accordingly	(7.4. Logging, Monitoring and Analytics (includes Alerting))	No					
11	sec. mon. 011	Monitoring /Audit	The Platform **must** Monitor and Audit logs from infrastructure elements and workloads to detected anomalies in the system components and take corrective actions accordingly	7.4. Logging, Monitoring and Analytics (includes Alerting)	No					
12	sec. mon. 012	Monitoring /Audit	The Platform **must** Monitor and Audit Traffic patterns and volumes to prevent malware download attempts	(7.4. Logging, Monitoring and Analytics (includes Alerting))	No					
13	sec. mon. 013	Monitoring	The monitoring system **must not** affect the security (integrity and confidentiality) of the infrastructure, workloads, or the user data (through back door entries).	(7.4.4. Logging, Monitoring, and Analytics (LMA) Framework)	No					
14	sec. mon. 015	Monitoring	The Platform **must** ensure that the Monitoring systems are never starved of resources		Yes					
15	sec. lcm.017	Audit	The Platform **must** Audit systems for any missing security patches and take appropriate actions	(7.2.2. Configuration Management)	No					

Compliance with Standards (RA-1 Section 2.3.8.8)

	Ref #	RA-1 Sub-Category	Description	RA-1 Traceability	RI Applicable	RI Toolset	RI Notes	RC Category	RC Toolset	RC Notes
1	sec.std. 018	Standards	The Public Cloud Operator **must**, and the Private Cloud Operator **may** be certified to be compliant with the International Standard on Awareness Engagements (ISAE) 3402 (in the US: SSAE 16); International Standard on Awareness Engagements (ISAE) 3402. US Equivalent: SSAE16		No	NA				