MANRS+ Controls Ver. 20250204

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)	Ownership	Comments
			Routing Security			
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbor or originated by the CP that is invalidated by an existing RPKI ROA is discarded and not announced to other BGP neigbours.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Verify that all RPKI setup is documented, including the validation workflow, which RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported, and how often these updates are published to their routers.[Self-declared][Audited]	Connectivity Provider (CP)	Efficacy of RS-01 depends on the implementation of controls RI-01 and RI-03 by the Enterprise Customers (EC).
Routing Security	Prefix Filtering of Customers	RS-02	In cases where RPKI Route Origin Validation cannot be effectively applied (e.g. no matching ROA is found), announcements received from a direct customer and its customer cone (if exists) are filtered using a whitelist (permit-list) generated from the IRR or by other means. Exception is the cases where unless the number of aggregated prefixes from a customer exceeds 1000 (discuss).	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. In case these cases happen on intrafaces that excluded from the requirement, verify that the number of aggregated prefixes exceeds 1000 (discuss) [Measured][Audited] 2. Check that the "Permit-list" prefix filtering is performed for all customers 3. Verify that the process for configuring new customer connections is documented and includes description of how the customer prefix-lists are generated and applied, how they are validated, and how often these prefix-lists are published to their routers. [Self-declared][Audited]	CP	Efficacy of RS-02 depends on the implementation of controls RI-02 and RI-03 by the Enterprise Customers (EC).
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-03	The CP implements filtering permitting only ASNs for a direct customer and its downstream customers (if exist) to originate announcements. The set of permitted ASNs is obtained from an AS-SET in an IRR or by other means.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured][Audited] 2. Verify that the Customer AS set is manintained [Measured][Audited] 3. The process for configuring new customer connections is documented and includes description of how the filter list of ASNs of the customer and its downstream customers (if exist) is build, how it is validated, and how often this filter is published to the routers. [Self-declared][Audited]		
Routing Security	Assistance with RPKI or IRR maintenance for a customer	RS-04	Assist a customer with implementing controls RI-01, RI-02 and RI-03.	1. Examine a documented list of the RPKI and IRR maintenance operations that the provider can perform at customer's request on their behalf.[Self-declared][Audited]	CP	
Routing Security	Prevent route leaks	RS-05	Route leaks are mitigated by using a peerlock technique (describe, or provide a reference)	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine documentation, which includes information about the technical architecture and processes of maintaining the control [Self-declared][Audited]	CP	
Routing Security	Filtering of bogons	RS-06	Bogon announcements are not propagated to BGP neighbours	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] For the purpose of this metric, the bogons are defined as follows: a. Pv4: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml b. IPv6: https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml c. ASN: https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml 2. Examine documentation, which includes information about the technical architecture and processes of maintaining this control. [Self-declared][Audited]	CP	
Routing Security	BGP session protection	RS-07	Measures are taken to ensure security of the BGP sessions with the neighbours	1. Check that CP's IP ranges do not appear on the Shadowserver reports https://shadowserver.org/what-we-do/network-reporting/accessible-bgp-service-report/ https://shadowserver.org/what-we-do/network-reporting/open-bgp-service-report/ [measured] 2. Examine documentation, which includes information how controls specified by RFC 7454 are implemented [Self-declared][Audited]		
			DDoS Attack Mitigation			
DDoS Attack Mitigation	Detection of volumetric DDoS attack traffic	DA-01	Ingress and egress traffic can be monitored for a set of IP addresses and malicious traffic can be detected and reported.	1. Examine documentation describing detection capabilities and its parameters. The documentation should demonstrate: - capabilities for detecting and reporting egress attack traffic at the customer-facing PE [mandatory] - capabilities for detecting ingress attack traffic at the PE from all neightbours [optional] - capabilities for reporting ingress attack traffic at the customer-facing PE [optional] [Self-declared][Audited]	CP	
DDoS Attack Mitigation	Rate limiting of malicious traffic	DA-02	Attack traffic can be rate limited.	1. Examine documentation describing rate limiting capabilities and its parameters. The documentation should describe which points in the network are capable of rate-limiting attack traffic. This should include filtering options available, such as source address, destination address, port, protocol, and interface. [Self-declared][Audited]	CP	

DDoS Attack Mitigation	Scrubbing of malicious traffic	DA-03	Malicious traffic can be scrubbed and clean, legitimate traffic is delivered to the customer. A corresponding service offering is available.	1. Examine documentation describing scrubbing capabilities and its parameters. The documentation should: - describe which points in the network are capable of attack scrubbing (transit, peering, customer), along with policy details on how this may be utilized by a customer; - demonstrate that a corresponding service offering is available. [Self-declared][Audited]	CP	
DDoS Attack Mitigation	Customer-triggered DDoS attack prevention	DA-04	DDoS mitigation capabilities are implemented by a CP and a customer is able to request specific actions from a CP using network protocols	1. Check metrics from the measurement system for the positive tests of RTBH- or FlowSpec-based filtering. [Measured] 2. Examine documentation, which should the description of signaling mechanisms for customer-initiated DDoS attack mitigation (e.g. RTBH, FlowSpec), including its capabilities and its parameters [Self-declared][Audited]	CP	
Anti-spoofing Protection						
Anti-spoofing Protection	Source address validation	AS-01	CP implements sufficient controls to prevent traffic with spoofed source IP addresses from its direct customers and the CP itself forwarded to other networks	1. Check for a negative Spoofer test from a customer network (Alt: Check metrics from the measurement system confirming ingress source address validation) [Measured] 2. Examine documentation, which includes information about the technical architecture and processes of maintaining this control. [Self-declared][Audited]	CP	
Anti-spoofing Protection	Mitigation of spoofed traffic	AS-02	CP has capability for tracing malicious spoofed traffic back to its source	1. Check that the CP has deployed tools to support this capability. Tools must include methods for collecting records of traffic (e.g. netflow) to perform real-time and historical forensics on traffic entering and traversing the network. The records must include data that defines which interfaces the traffic is entering the network. [Self-declared][Audited]	CP	
Maintaining Routing Information						
Maintaining Routing Information	ROA registration	RI-01	1. ROAs cover all announcements to other BGP neighbours originated in the CP network 2. Published ROAs do not invalidate legitimate announcements	1. Compare route announcements using externally visible the BGP information (RIS, RouteViews) with the ROAs in the RPKI repository. Ensure that all announcements are properly covered. [Measured] 2. Check that none of the ROAs invalidates legitimate announcements originated by the CP. [Measured] 3. Examine the documentation to ensure that ROA maintenance follows best practices. [Self-declared][Audited]	Shared	Corresponding control - RS-03
Maintaining Routing Information	IRR route object registration	RI-02	1. IRR objects are published in the RIR IRR authoritative for the corresponding address space 2. IRR route objects cover all announcements originated in the CP network 3. IRR route objects cover announcements originated in the customer cone networks 4. There are no conflicts among the RIR IRRs and RPKI as far as route objects related to CP announcements are concerned	1. Compare route announcements using externally visible the BGP information (RIS, RouteViews) with the IRR registrations. Ensure that all announcements are properly covered. [Measured] 2. Check that the route object corresponding to an announcement is registered in the correct IRR (the one authoritative for the corresponding address block) and there are no conflicting records in the RPKI. [Measured] 3. Examine the documentation to ensure that ROA maintenance follows best practices. [Self-declared][Audited]	Shared	Corresponding control - RS-03
Maintaining Routing Information	AS-SET registration	RI-03	1. AS-SET uses the IRR::ASN:AS-NAME notation and lists the CP customer cone members (ASNs and AS-SETs) 2. AS-SET is registered in the PeeringDB and the RIR IRR authoritative for the CP ASN.	1. Check the AS-SET records in the Peering DB and the IRR hosting the ASN and ensure they are in the proper format.[Measured]	Shared	Corresponding control - RS-03
Facilitate global operational communication and coordination						
Facilitate global operational communication and coordination	Valid contact email	GC-01	1. Contact information is publicly available 2. Contact email is operational	1. Check that contact information is available in one of the databases (RIR/NIR or PeeringDB) [Measured] 2. Check the address is valid and responsive by sending a test e-mail and expecting a human response within predefined time. [Measured]	CP	
Security services						
Security services	Secure configuration	SS-01	1. Secure configuration for customer devices facing the provider is available and the deployment can be assisted on request	1. Check that secure configuration templates (e.g. CIS benchmarks) are available [Self-declared][Audited] 2. Examine documentation for the process of deployment of such configurations on customer's request. [Self-declared][Audited]	Shared	
Security services	Monitoring and reporting	SS-02	1. Monitoring and reporting if a customer announcement is invalidated by ROAs 2. Monitoring and reporting if a customer announcement is being hijacked (or more general - if the routing policy was violated) outside the control of the connectivity provider	1. Examine documentation for the monitoring and reporting service. [Self-declared][Audited]	Shared	
Security services	Assistance in registration	SS-03	1. Offer assistance in the registration of customer's routing information in the IRR and RPKI systems.	1. Examine documentation of the registration assistance service.[Self-declared][Audited]	Shared	
Supply chain transparency (experimental)						
Supply chain transparency	ASPA registration (when available, experimental requirement)	ST-01	1. All upstream providers are documented in RPKI using ASPA objects	1. Check the RPKI for the existence of ASPA objects and corroborate this with AS relationship data (e.g. CAIDA AS relationship, or RIPEStat)		This is just a suggestion for a future control