Strengthening a business case for routing security: MANRS+

Is your connectivity provider a threat vector or the first line of defense?

GLOBAL CYBER ALLIANCE™

Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats. Otherwise - they are part of the problem.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can’t charge extra for it.

A secure routing system benefits all. But even if you do everything right, your security is still in the hands of other networks.

This is a collective action problem.

A collaborative approach:

Mutually Agreed Norms for Routing Security (MANRS)

An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

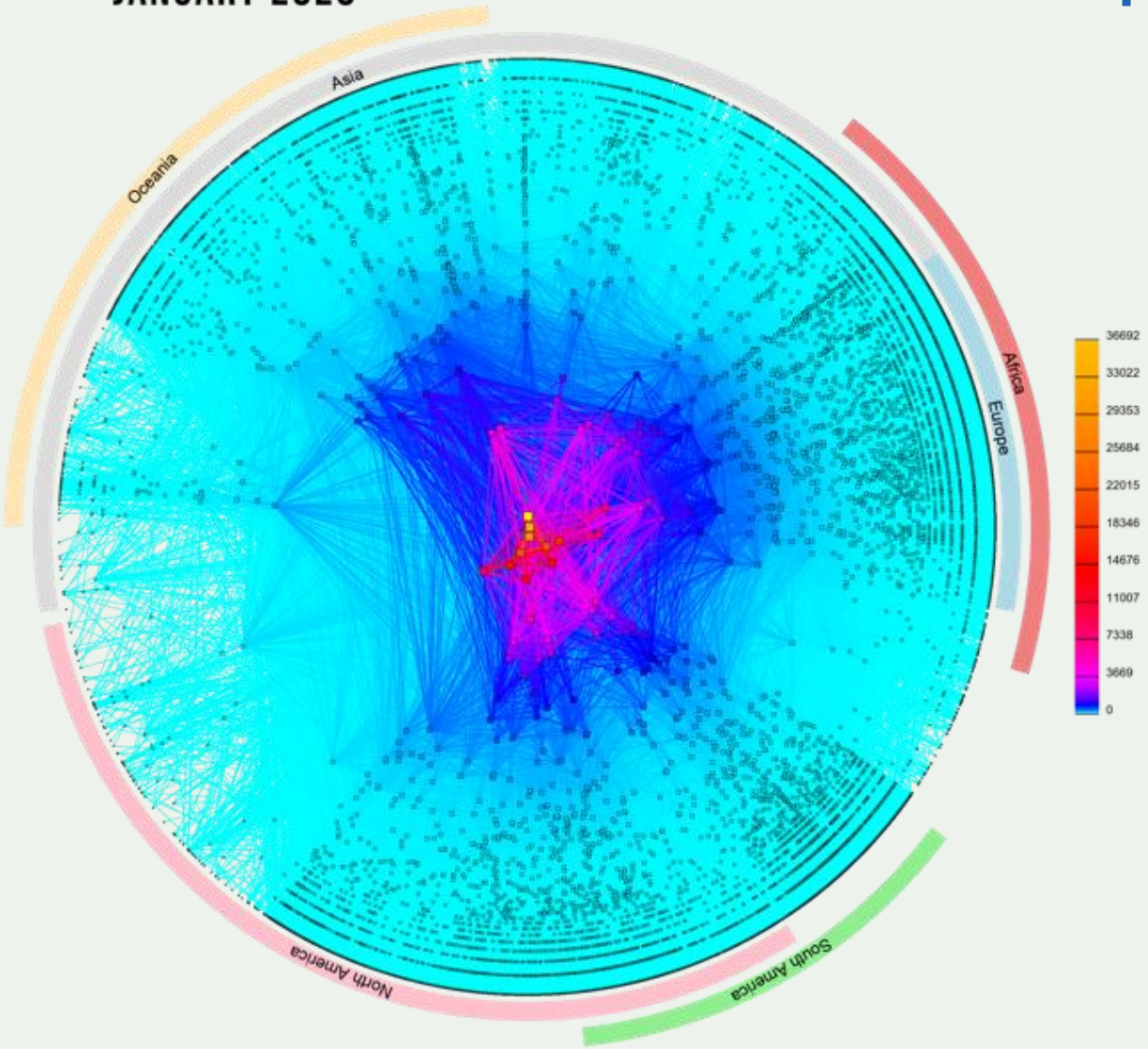
Demonstrated commitment by the participants

- Measured by the Observatory and published on https://www.manrs.org

The MANRS (and routing security) business case

- **Protecting own network** by improving security processes and deploying essential controls
- **Improving security of the global routing system** (overcoming the collective action problem), because
  - routing security is a sum of all contributions
  - this is a way to promote a new baseline
  - a community has gravity to attract others
- **Gaining competitive advantage** by responding to **customer demands?**

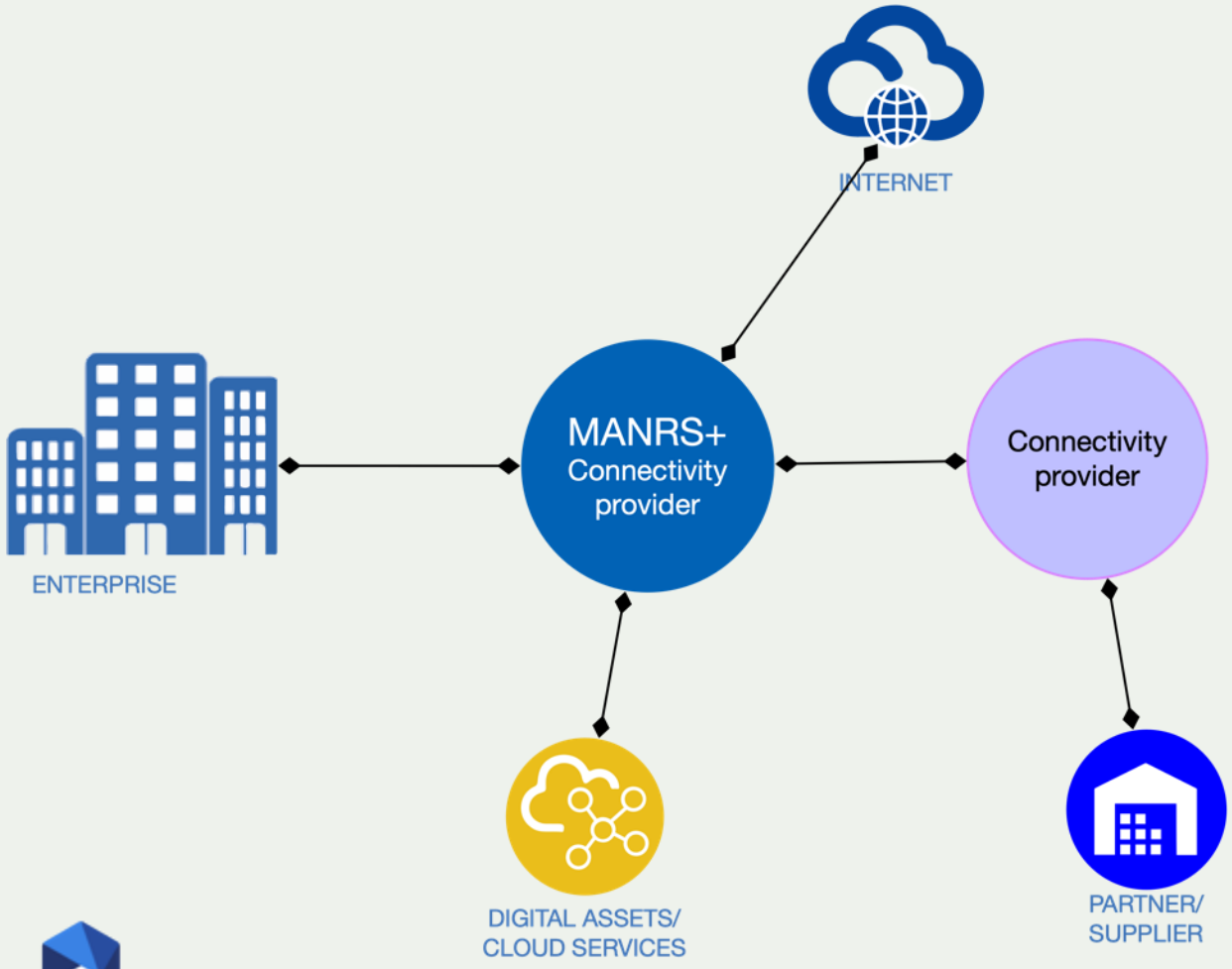
The real Internet



https://www.caida.org/

MANRS

Traffic security for enterprises – a smaller Internet

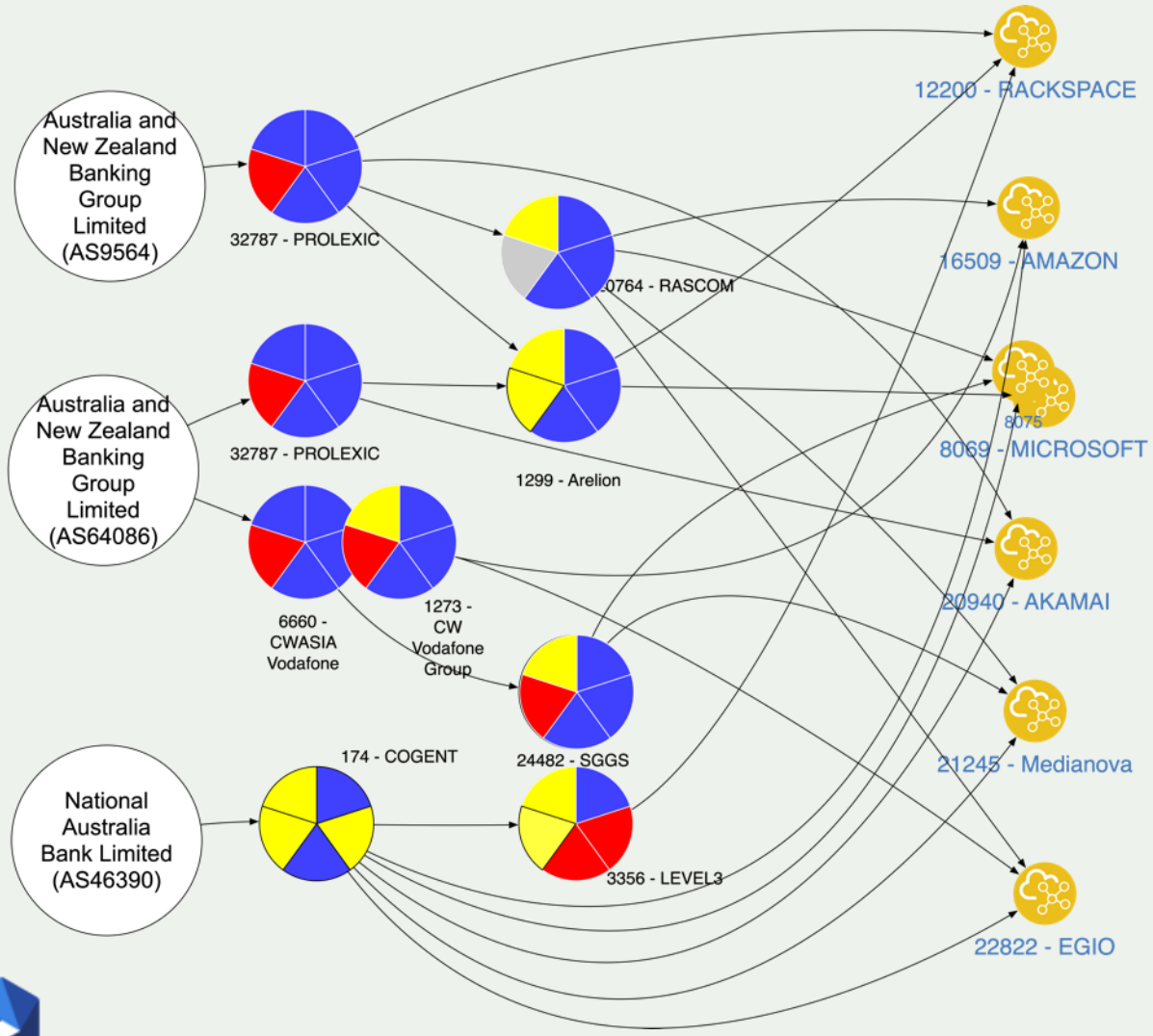


Enterprise's connectivity provider is the first line of defense against routing incidents.

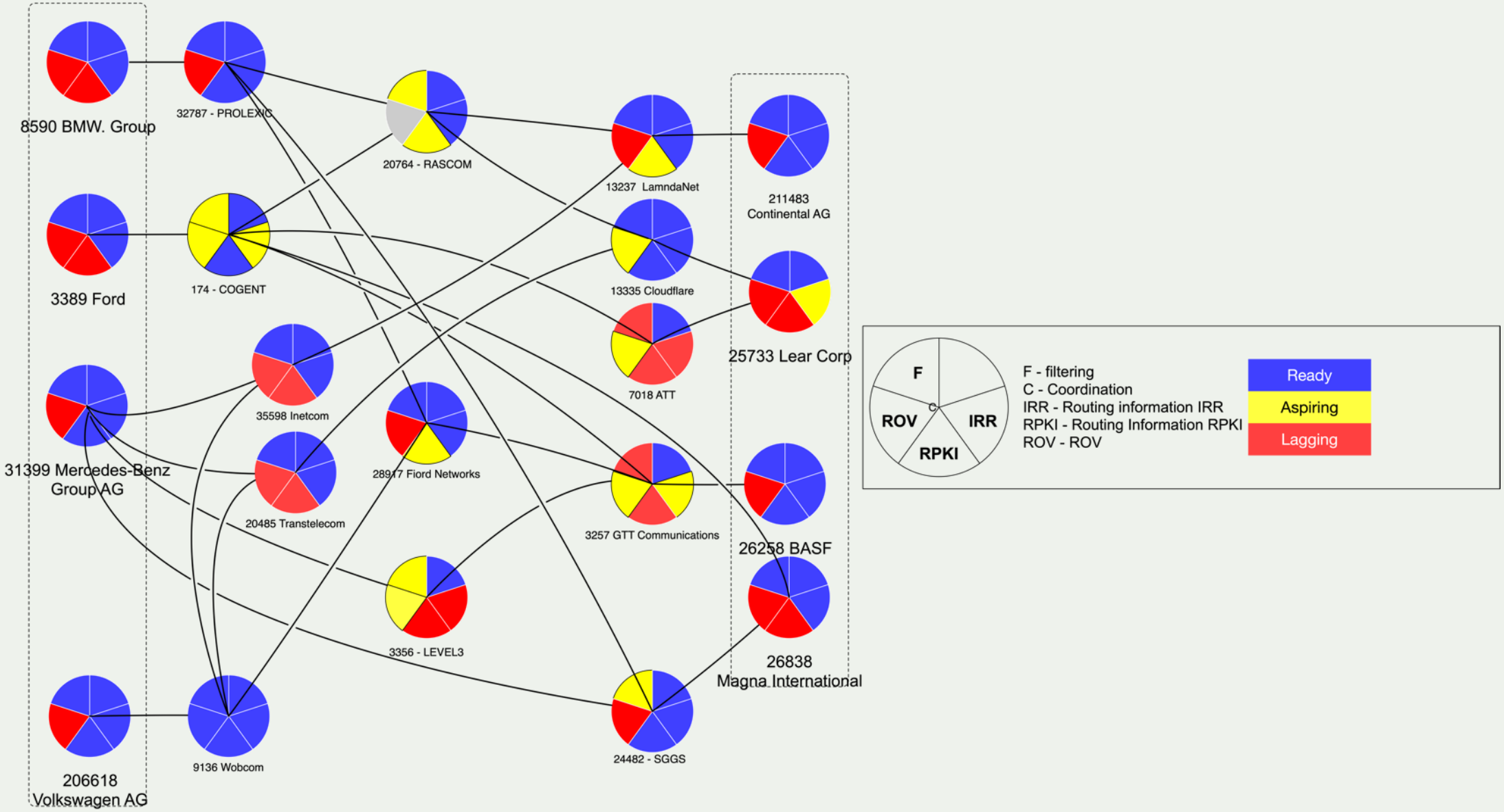
Enterprise can reduce risk by implementing the MANRS actions.

A strong and reliable tie with the connectivity provider(s) can achieve much more – secure the company supply chain.

Supply chain example: AU banking



Supply chain example: Automotive (B2B)



Routing security as part of supply chain security

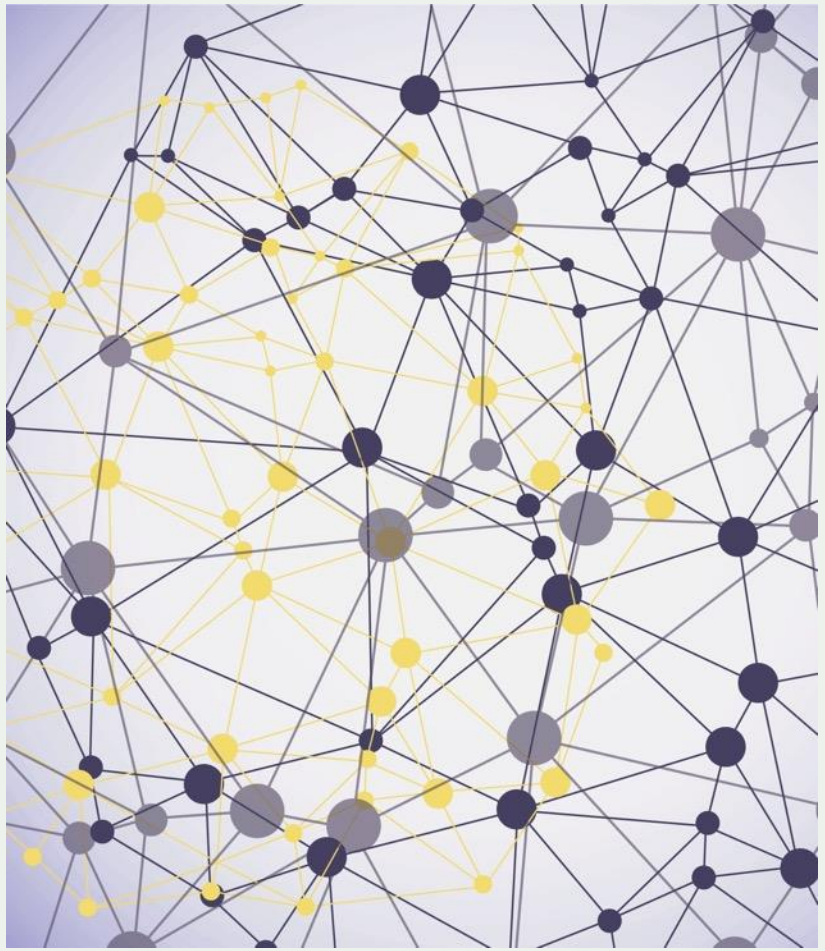
85% of all ASes are origin-only networks. They fully depend on their connectivity provider for accessing their external digital assets and the Internet.

However, origin-only networks, mostly “enterprises” can contribute to a better routing security by:

1. Enterprises **implementing** routing security best practices in their network infrastructure.

2. Enterprises **demanding** proper routing security controls from their connectivity and cloud providers.

Is your connectivity or cloud provider the first line of defense, or the weakest link?



MANRS+

- A framework for routing security, essential part of supply chain security
- Focus on the demands of enterprise customers in various industry sectors
  - *Extended set of requirements, covering a broader set of risks related to routing and traffic security*
- Conditioned to be included in/referenced from common infosec frameworks
  - *Stronger and more detailed requirements enforcing best practices in traffic security*
  - *High level of assurance of conformance. This includes more profound technical audit and process audit.*
  - *Developed in an transparent and inclusive manner – Standard Development Process*

What should enterprises require from their connectivity provider? MANRS+ Requirements (The Controls Matrix)

Routing Security
7 Controls

DDoS Attack Mitigation
4 Controls

Anti-spoofing Protection
2 Controls

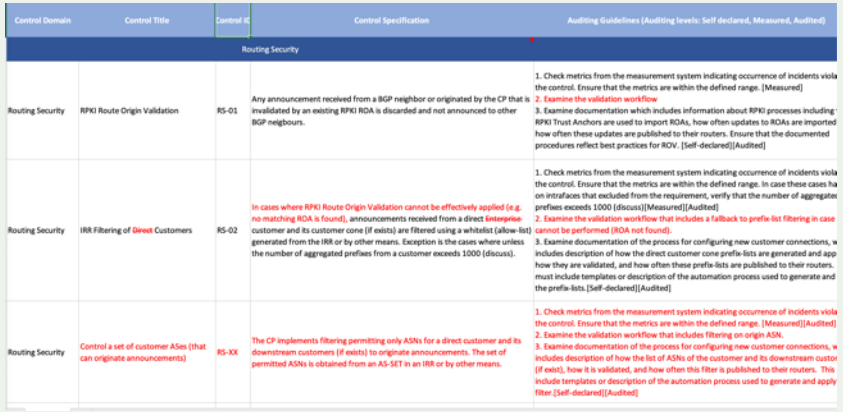
Maintaining Routing Information
3 Controls

Global Communication
1 Control

Security Services
3 Controls

Current status

- Work is done by the MANRS+ WG:
  - https://manrs.org/about/manrs-working-group/
  - The WG meets on Zoom, ongoing discussions are on the mailinglist
  - Anyone can join this effort → contact@manrs.org
  - The final draft of the Controls Matrix is ready

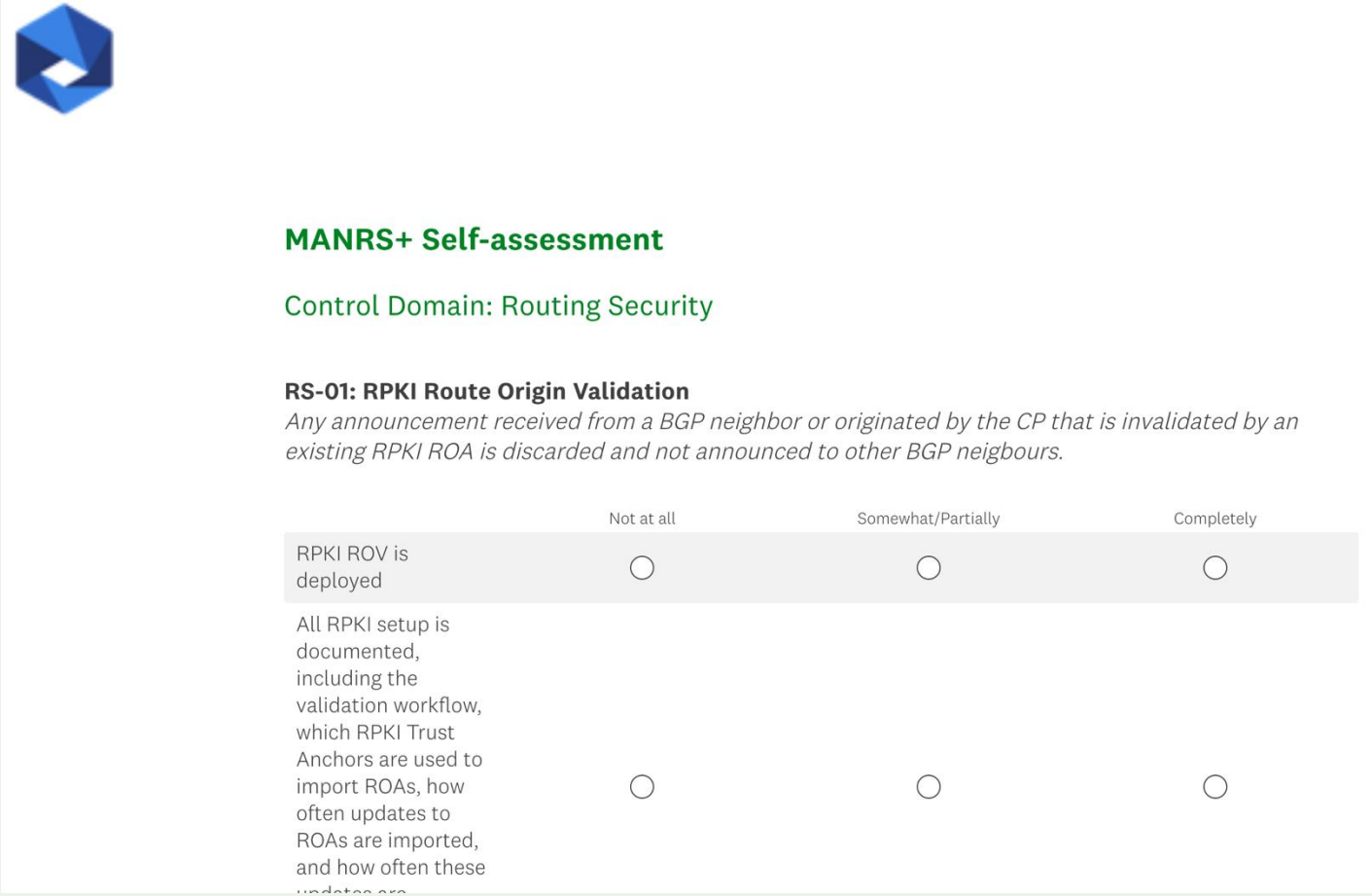


Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)
Routing Security				
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbor or originated by the CP that is invalidated by an existing RPKI ROA is discarded and not announced to other BGP neigbours.	1. Check metrics from the measurement system indicating occurrence of incidents viola the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine the validation workflow 3. Examine documentation which includes information about RPKI processes including RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported how often these updates are published to their routers. Ensure that the documented procedures reflect best practices for ROV. [Self-declared][Audited]
Routing Security	IRR Filtering of ~~Direct~~ 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 ~~Enterprise~~ customer and its customer cone (if exists) are filtered using a whitelist (allow-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 viola the control. Ensure that the metrics are within the defined range. In case these cases ha on intrafaces that excluded from the requirement, verify that the number of aggregate prefixes exceeds 1000 (discuss)[Measured][Audited] 2. Examine the validation workflow that includes a fallback to prefix-list filtering in case cannot be performed (ROA not found). 3. Examine documentation of the process for configuring new customer connections, includes description of how the direct customer cone prefix-lists are generated and app how they are validated, and how often these prefix-lists are published to their routers. must include templates or description of the automation process used to generate and the prefix-lists.[Self-declared][Audited]
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-XX	The CP implements filtering permitting only ASNs for a direct customer and its downstream customers (if exists) 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 viola the control. Ensure that the metrics are within the defined range. [Measured][Audited] 2. Examine the validation workflow that includes filtering on origin ASN. 3. Examine documentation of the process for configuring new customer connections, includes description of how the list of ASNs of the customer and its downstream custo (if exist), how it is validated, and how often this filter is published to their routers. This include templates or description of the automation process used to generate and apply filter.[Self-declared][Audited]

Self-assessment Survey

Objectives:

- To evaluate the clarity and feasibility of the audit requirements in the Control Matrix
- To evaluate readiness of your organisation to meet these requirements.
- Basis for the future application form



MANRS+ Self-assessment

Control Domain: Routing Security

RS-01: RPKI Route Origin Validation

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.

	Not at all	Somewhat/Partially	Completely
RPKI ROV is deployed	○	○	○
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	○	○	○

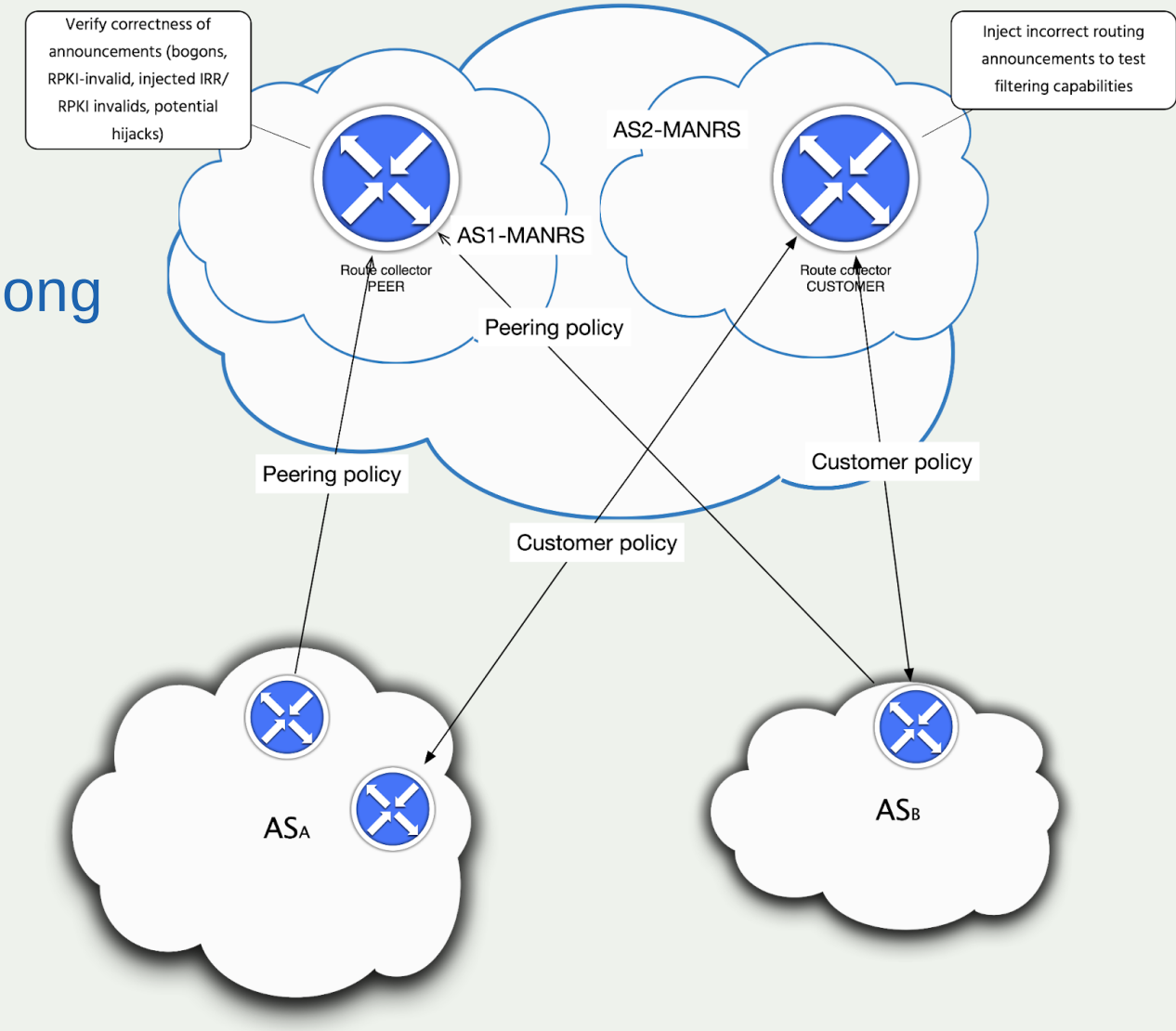
Futurte work:

Gather interested organizations, both among connectivity providers and enterprises

Prototype and deploy the enhanced measurement infrastructure

Work on inclusion in common infosec frameworks

E.g. M3AAWG Internet Routing Security Profile based on NIST CSF



Get involved.

contact@manrs.org

manrs.org

GLOBAL CYBER ALLIANCE™