OTORIO

RAM^2

NISG - Compliance enablement

Introduction

NISV

NISV is the official Austrian regulation of the Network and Information System Security Ordinance that defines concrete network and information security requirements for providers of essential services within the framework of the Network and Information System Security Act (NISG). NISG and NISV address essential services in multiple sectors, including:

1. Energy
   a. Electricity - generation, distribution and transmission
   b. Oil - production, storage, transport, refining
   c. Gas - production, storage, transport, marketing, distribution
2. Transport sector
   a. Air transport - Commercial air transport, Airport, Air traffic control,
   b. Rail transport - infrastructures, rail transport services,
   c. road transport
3. Banking
4. Financial market infrastructures sector
5. Health sector
6. Drinking water supply sector
7. Digital infrastructure

NIS 2 Directive - https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

NISG - https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2018_1_111/ERV_2018_1_111.pdf

NISV - https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2019_2_215/ERV_2019_2_215.pdf

NISV detailed requirements according to NISV Annex 1 -

https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf

RAM^2 - Continuous OT Cyber Risk Management

Prescriptive protection for operational environments

OTORIO's RAM^2 provides continuous operational risk monitoring, assessment and management to automate and contextualize the entire operational security lifecycle. It orchestrates data from cross domain sources to deliver consolidated visibility and context-aware, impact-driven prioritization. By providing prescriptive, expert defined risk mitigation guidance, the platform empowers OT security practitioners to proactively manage cyber risks on their digital transformation journey, while meeting changing business and market requirements.

OTORIO RAM^2 is used today by operational organizations including customers in the Energy sector (Electricity, Oil & Gas), Smart transportation (including airports), Manufacturing and more.

OTORIO RAM^2 - NISG compliance enablement

The following table details OTORIO's RAM^2 capabilities that enable essential services and operators of OT environments to be compliant with the NISG requirements as detailed in NISV - Annex 1 - Security measures.

Annex 1 - Security measures	
Requirement	**OTORIO RAM^2**
2. Governance and risk management	
1.1 Risk Analysis NIS regulation: A risk analysis of the network and information systems must be carried out. In doing so, specific risks are to be determined on the basis of an analysis of the operational effects of security incidents and evaluated with regard to the great importance of the operator of essential services for the functioning of the community. The operator carries out a risk analysis and updates it regularly. The analysis identifies those network and information systems that the operator is responsible for providing of the Essential Service (or Services) and the associated risks. The risks include all circumstances or events that have a potentially adverse impact on the security of the identified network and information systems and that can be identified with reasonable effort. This analysis forms the basis for focusing and prioritizing security measures and activities. Carrying out the risk analysis includes the above-mentioned ongoing update as part of a continuous improvement process (CIP). When updating the analysis, new threats, the loss of effectiveness of implemented measures and changes in the risk situation, e.g due to changes in the system architecture.	● RAM^2 provides continuous monitoring and risk assessment. ● Impact driven prioritization of risks. ● Assessment based on operational context and related to the operational processes that may be affected by disruption to assets' performance. ● Risk assessment reports generated from the system. ● Option for on-demand assessment, including for areas which are not connected to the network. ● Identifying security gaps and vulnerabilities, assessing the security posture and attack surface. ● Detecting threats and prioritizing mitigation actions ● Comprehensive coverage of OT, IT and IoT assets in the operational environment. ● Practical mitigation steps for continuous improvement process. Suggesting alternatives to patching which may not be an option in OT networks (for legacy systems, for devices that cannot be shut down). ● Reflecting trends of changes in risk over time. ● Risk indicators can be collected from multiple data sources in the environment and are not limited to network monitoring (safe active querying, passive network monitoring, EDR, Firewall, DCS, PLCs and more). Data is correlated to identify potential risks.
1.2 Security Policy NIS Regulation: A security policy must be created and updated periodically. The operator creates, maintains and updates a security guideline that defines strategic security goals, describes risk management and refers to all other relevant specific security requirements (directives, guidelines, etc.)	● RAM^2 provides out-of-the-box best practices policy monitoring and compliance audit with several standards (e.g. IEC 62443-3, NERC CIP, NIST). ● Users can control and update the policies.
1.3 Review plan of network and information systems NIS regulation: The implementation of the periodic review of network	● RAM^2's attack graph analysis maps the network topology based on both firewall rules and open ports (potential access) and passive network monitoring (actual traffic).

and information system security is to be planned and specified. According to the defined inspection plan, the operator independently inspects the identified network and information systems. Checks of the network and information systems are carried out as part of the check plan and depending on the risk analysis. These checks aim to validate the application, effectiveness and adequacy of the defined security measures. The operator provides an overview and continuously updated documentation of the tests carried out.	● Identifies protocols in use. ● Monitors and reports communication between assets and potential breaches, including between operational processes. ● RAM^2 also provides recommendations for hardening of the network by restricting specific communication or hardening of specific nodes.
1.4 Resource Management NIS regulation: All resources required to ensure the functionality of the network and to ensure information systems are in terms of short, medium and plan and ensure long-term capacity requirements. The operator ensures the short, medium and long-term availability of all human, financial and technical resources required for the functionality of the network and information systems.	● RAM^2 discovers and identifies OT, IT and IoT assets in the network. ● Assets are assigned to operational processes in the organizational hierarchy to assess the impact at the organizational level and support decision making for resource allocation according to scope, impact and risk levels.
1.5 Information security management system review NIS regulation: The periodic review of the information security management system must be defined and carried out. The operator uses a series of indicators and methods to evaluate compliance with its security guidelines. Indicators may relate, for example, to the adequacy and effectiveness of the operator's risk management, the maintenance and operation of resources in safe conditions, user access rights, and authentication of access to resources and resource management	● RAM^2 provides indicators regarding the risk of assets and operational units at all levels, as well as compliance assessment from the single asset level, to machine and entire operational environment. ● It gives transparency regarding the risk trend over time. ● RAM^2 assesses the status and utilization of existing security controls (e.g. Firewall configurations, user configurations in the Active Directory, security configurations of assets and operational systems).
1.6 Human Resources NIS regulation: Safety-relevant aspects must be taken into account and implemented in the human resources processes. The operator ensures that employees are trustworthy and aware of their responsibilities. The operator also ensures that employees are qualified for the roles assigned to them. There is a corresponding training and education program for further and advanced training in safety-related subject areas. All employees are made aware of security issues and a special security training program for employees with specific responsibility for network and information systems is carried out.	NA
2. Dealing with service providers, suppliers and third parties	

2.1 Relationships with Service Providers, Suppliers and Third Parties NIS regulation: Requirements for service providers, suppliers and third parties for the operation of a secure access to and access to network and information systems defined and periodically reviewed. The operator creates an overall picture of its ecosystem, including service providers and suppliers with contractual relationships, as well as third parties, especially those who have access to or manage the network and information systems. The purpose of this overall picture is to identify and assess risks and dependencies arising from the relationships with the service providers, suppliers and third parties. In order to carry out this assessment, the person responsible takes at least the following questions into account: • Maturity: What technical capabilities do the service providers, suppliers and third parties have in relation to cybersecurity? • Trust: Can I assume that the intentions of the service provider, supplier and third party towards me are trustworthy and that they themselves are reliable? • Access level: What access rights do service providers, suppliers and third parties have to network and information systems? • Dependence: To what extent is the relationship with service providers, suppliers and third parties decisive for the activity?	● Using OTORIO's remOT solution for operational secure remote access, customers can secure, control and govern the access of third parties, allowing access to each user only to the assets needed, using the specific protocols needed, adopting a zero-trust approach, with maximum simplicity and scalability.
2.2 Service Level Agreements with Service Providers and Suppliers NIS regulation: The performance agreements with service providers and suppliers must be checked and monitored periodically. The operator establishes a policy for its relationships with service providers and suppliers in order to minimize the identified risks. A special focus is placed on the interfaces between their network and information systems and those of the operator. In general, security requirements must be identified and defined for network and information systems operated by service providers. The operator uses service level agreements (SLA) and/or verification mechanisms to ensure that its service providers and suppliers also implement appropriate security measures in order to meet the security requirements of the operator. Together with its service providers and suppliers, the operator defines reaction and recovery processes after (security) incidents and checks them periodically.	NA
3. Security Architecture	
3.1 System Configuration NIS regulation:	● RAM^2 automatically collects the configurations of the network, security controls and security related configurations of industrial systems, to document

Network and information systems must be configured securely. This configuration must be documented in a structured manner. The documentation must be kept up to date. The operator only uses resources (e.g. services and devices) that are necessary for the operation of the network and information systems. During installation and throughout the life cycle, the operator follows a system hardening approach. In addition, the operator ensures that the configuration of all relevant components is documented. The operator updates this documentation regularly.	and manage the data. ● The data is used to audit for compliance with security standards. ● RAM^2 provides recommendations for hardening of the operational environment based on the documented configurations.
3.2 Assets NIS regulation: Assets related to network and information systems are to be analyzed and documented in a structured manner. The operator creates a suitable concept for the management of assets (assets) for the identification, classification and inventory of IT processes, systems, components as well as software platforms/licenses and applications. In the inventory, clear roles and responsibilities are defined for each asset and classified according to their criticality. Among other things, the inventory supports the rollout of updates and patches and, if necessary, enables a determination of which components are affected by new security problems or vulnerabilities.	● RAM^2 ingests assets data from cross-domain sources in the operational environment. It augments the data, enriches it and provides a complete and accurate inventory and asset management capability. ● RAM^2 enables the export of reports regarding the asset inventory, and integration with other systems on the customer's network, as a single south of truth regarding the assets in the OT network. ● Assets are classified in the system according to type. ● The platform provides visibility into basic asset identifiers (IP, MAC, vendor, catalog number, OS, serial. ● It provides a list of installed software, interfaces, security configurations, connected devices, host FW configurations, installed patches, and more. ● Depending on the integrated systems, it also provides related operational processes. ● This accurate inventory is used for accurate mapping to publicly known vulnerabilities (CVEs) and identification of security gaps.
3.3 Network Segmentation NIS regulation: Networks must be segmented within the network and information systems depending on the protection requirements. The operator separates its systems physically or logically depending on the protection requirement and classification in order to contain the effects of (security) incidents within its systems. The operator only permits connections between systems with different protection requirements and different classifications that are of significant importance for the functioning of the network and information systems. For such interfaces (e.g. interfaces between the network and information systems of suppliers and customers), the operator documents appropriate security mechanisms and implements them. This includes, among other things, processes and procedures for secure access, remote access, monitoring or data exchange.	● RAM^2 analyzes firewall configuration to identify gaps in the segmentation between the OT and the IT or the Internet. It provides prescriptive instructions for risk mitigation by doing configuration changes. ● RAM^2 leverages the data it collects from all sources (including passive network monitoring, firewall configurations, Safe active querying, EDR, DCS, and all other integrations available) to create a Cyber Digital Twin that represents the assets and connections between them, vulnerabilities and exposures, as well as the assets impact and relation to operational processes. Based on the Cyber Digital Twin the platform generates an attack graph, and calculates attack vectors to assets within the network. This way it identifies potential breaches between the network and the IT, and prioritizes the hardening and restriction of the most critical vectors. ● The information is available within the platform's UI and in reports.
3.4 Network Security NIS regulation:	● In addition to identifying potential gaps in the external attack surface, RAM^2 uses its Cyber Digital

Security within the network segments and the interfaces between the network segments must be guaranteed. The operator filters incoming and outgoing network traffic and limits it to what is absolutely necessary for the functioning of the network and information systems. The operator also filters network traffic within the network, banning any network traffic that is not necessary for the functioning of its systems and can facilitate potential attacks. To do this, the operator defines and updates the filter rules regularly by network address, port number, protocol, etc.	Twin to identify actual and potential connections between different operational processes within the network. It helps customers assess their internal segmentation, identify communication using unsecure protocols and connections that allow access to vulnerable assets. By following a zero trust approach, RAM^2 empowers operators to restrict communication and ensure only absolutely necessary interfaces are enabled.
3.5 Cryptography NIS regulation: Confidentiality, authenticity and integrity of information must be ensured through the appropriate and effective use of cryptographic procedures and technologies. The operator establishes policies and procedures for the use of cryptography and key management to ensure their appropriate and effective use to protect the confidentiality, authenticity and/or integrity of information and systems in its network and information systems.	● Unlike IDS products, RAM^2's passive network monitoring monitors metadata of the traffic and does not rely only on deep packet inspection of the network traffic, which requires the communication to be unencrypted and unsecure by design. ● To complement and extend the asset identification, RAM^2 uses its proprietary Safe Active Querying capabilities, and integrates with a variety of proprietary (e.g. SNMP Traps) and third party sources that enrich the data and detect threats.
4. System Administration	
4.1 Administrative Access Rights NIS regulation: Administrative access rights are to be assigned in a restricted manner according to the principle of minimum rights. These allocations must be checked periodically and adjusted if necessary. The operator sets up dedicated and personalized accounts for the administration - insofar as this is supported by the system - which may be used for the purpose of installation, configuration, administration, maintenance, etc. These accounts are documented on a constantly updated list and checked in a regular review process, with such a list also being maintained for non-administrative accounts. The administrative authorizations granted are limited to the functional and technical area of responsibility of the respective administrative user account. These user accounts are only used for the purpose of administration itself and for connecting to administrative systems. Use for non-administrative activities is prohibited. When allocating administrative accounts, requirements for the separation of duties are taken into account and administrative activities are logged.	● RAM^2 identifies the use of default credentials in assets to proactively secure assets and prevent use by unauthorized employees, service providers or malicious parties..
4.2 Systems and Applications for System Administration NIS regulation: Systems and applications for system administration are	● OTORIO's remOT solution provides secure remote access and allows access only to specific assets using predefined protocols. It prevents the use of a jump box for access by third parties, and secures authorized only communication.

to be used exclusively for activities for the purpose of system administration. The security of these systems and applications must be guaranteed. Only systems intended for this purpose by the operator or service provider are used to carry out administrative activities. Hardware and software used for administrative activities are managed and securely configured by the operator or, if applicable, by the service provider that the operator has authorized to carry out administrative activities. Administrative systems are used exclusively to carry out administrative activities and are not used for other activities. In particular, they are not used to access the Internet. Under no circumstances should users connect to a system used for administrative activities via a software environment that is used for functions other than administration. With regard to the use of so-called "jump servers"/"jump hosts" to carry out administrative activities, see Chapter 6.2 Remote access. The operator sets up a dedicated logical or physical network to connect the administrative systems with the systems to be managed. Secure, state-of-the-art protocols, authentication and encryption mechanisms are used for administrative activities.	
5. Identity and Access Management	
5.1 Identification and Authentication NIS regulation: Procedures must be implemented and technologies used that ensure the identification and authentication of users and services. For identification, the operator sets up unique accounts for users or for automated processes that need to access network and information systems according to a defined and documented procedure. Accounts that are not used or no longer required must be deactivated. A regular review process is set up for this purpose. For authentication, the operator protects access to resources of its network and information system by users or automated processes with a secure authentication mechanism. The operator defines the rules for managing the authentication data. Whenever necessary, users regularly change their authentication credentials according to defined policies. In particular, the operator changes the standard authentication data installed by the manufacturer/supplier before putting a system into operation. The use of procedures for two-factor authentication is taken into account by the operator in its architecture and promoted in a targeted manner.	● RAM^2 integrates with Active Directory to analyze user configurations and identify vulnerable configurations such as users with no password, expired passwords, users that haven't been used for more than 6 months and more. ● The platform enables identification of admin users that access assets in the network. ● RAM^2 itself can be configured to be used with two-factor-authentication.
5.2 Authorization NIS regulation: Procedures must be implemented and technologies	

used to prevent unauthorized access to network and information systems. The operator only grants access rights to users or automated processes according to defined rules if their access is absolutely necessary for the fulfillment of tasks or the implementation of automated processes. Access rights are always granted using the defined rights request process, in which the separation of duties is taken into account accordingly. Measures are implemented to ensure compliance with the "need-to-know" principle or the minimum rights principle. The operator reviews these access rights at least once a year, examining the user accounts, their associated access rights and the corresponding systems or functionalities that are accessed with these access rights. The operator maintains and updates a list of privileged accounts (e.g. administrative accounts). The operator checks every possible change to a privileged user account to ensure that the access rights to systems and functionalities comply with the minimum rights principle and are appropriate for the use of the user account.	
6. System Maintenance and Operation	
6.1 System Maintenance and Operation NIS regulation: Procedures and procedures to ensure secure system operation of network and information systems must be introduced and periodically reviewed. The operator defines procedures and conditions under which the security of its network and information systems is ensured during operation. Among other things, a procedure is also defined for collecting information about vulnerabilities and associated patches that affect network and information systems and for taking the appropriate steps derived from this. A corresponding procedure can contain both manual and automatic components. No specific technical measure is explicitly specified, since the corresponding procedure depends on the system environment and risk assessment. The operator ensures that the system versions used are up-to-date from a safety point of view. The operator checks the origin and integrity of the respective system version before it is installed or updated and analyzes the technical and operational effects of this version on the network and information system in question. The operator ensures that components of the network and information systems are regularly serviced according to their maintenance intervals and logs the implementation.	● RAM^2 identifies vulnerabilities in assets within the network. It alerts on those alerts. The vulnerability mapping is based on OTORIO's vulnerability database that is maintained by OTORIO's research team. Updating the vulnerability database enables the detection of new vulnerabilities based on the asset fingerprints that are managed within the platform. ● RAM^2 identifies the assets attributes including firmware version. It also alerts on changes in the firmware. The platform does an accurate vulnerability mapping to reduce noise and alerts according to the asset identification and firmware version. ● RAM^2 suggests the required patch for remediation of vulnerabilities. However, it also provides step-by-step guidance for mitigation using alternatives to patching, which allows an immediate action even when patching is not an option (due to no maintenance window, legacy devices that do not have patches etc.). ● Assets are assigned to operational processes, can have business impact scoring, and can be viewed with respect to other assets that are connected to them. This allows the operator to assess the potential consequences of patching before committing the procedure.
6.2 Remote Access NIS regulation: Remote access is restricted according to the minimum rights principle and in terms of time limited to give. The	

remote access rights are to be checked periodically and adjust if necessary. The security of the remote access must be guaranteed. The operator establishes processes for managing remote access. In particular, he provides techniques that allow remote access to network and information systems only authorized according to the principle of minimum rights and for a limited time. Authentication for remote access is implemented using two-factor authentication. Any unauthorized access is prevented. For maintenance work that is carried out remotely, the operator ensures that all activities and operations are recorded and documented. All access by external persons can only take place under the control of the system manager. The use of so-called "jump servers"/"jump hosts", e.g. for carrying out administrative activities, is certainly possible. The configuration of the jump servers/jump hosts for use by employees who connect from a device from a network section with lower protection requirements or the use of security measures by those same users must comply with the specifications for remote maintenance by external parties.	
7. Physical Security	
7.1 Physical Security NIS regulation: The physical protection of the network and information systems, in particular the physical protection against unauthorized entry and access must be guaranteed. The operator prevents unauthorized physical access to, access to, damage to and interference with network and information systems. In particular, the operator creates a physical security concept including a corresponding definition of different security zones and defines procedures for the safe handling of visitors and external personnel (such as maintenance technicians, service providers, suppliers or third parties).	NA
8. Incident Detection	
8.1 Detection NIS regulation: Mechanisms for detecting and evaluating incidents must be implemented. The operator sets up a system for detecting security-related events. The sensors set up in the network and on system components are analyzing for this purpose the transmitted data, data streams, protocols and the behavior of individual systems or components themselves to detect events that may affect the security of network and information systems. This system must be set up in such a way that it covers at least all data flows exchanged between the operator's	● RAM^2 uses Edge devices to access different areas of the network and remote sites. ● It provides passive network capabilities to monitor the network traffic. This capability enables the mapping of the communication in the network, including protocols used, between assets and between operational processes. ● RAM^2 monitors the metadata of the communication, not using deep packet inspection (DPI), that would be limited in case of encrypted communication. ● RAM^2 extends its ability to detect suspicious behavior in the network by correlating data and events from multiple sources. It utilizes pattern-based detection to alert about

network and information systems and those of the suppliers and service providers. The operator defines default values for allowed system and network operations and expected data flows and activities.	security-related events and incidents. Some examples for integrations that are used for data collection include the passive network monitoring, safe active querying, SNMP notifications monitoring, Firewall logs, secure remote access, DCS, and more (See OTORIO's Platform integrations document for additional information). ● The correlated alerts generated by RAM^2 allow for an early detection of suspicious patterns, with full context (e.g. by automatically alerting on a pattern that indicates the existence of rogue device includes the discovery of a new asset, the fact that that asset is lacking an EDR agent as required, the triggering of an ARP scan from that asset followed by a communication from that asset using an unsecure protocol to a vulnerable asset with high impact, that results in a firmware change on the target asset).
8.2 Logging and Monitoring NIS regulation: Mechanisms for logging and monitoring, especially for the provision of the essential service essential activities and processes, are to be implemented. The operator implements mechanisms in its network and information systems logging and monitoring. The logging includes, among other things, the application servers, System and network infrastructure servers, security technologies and systems, engineering and maintenance stations of industrial systems, network equipment and administrative Workstations that support critical activities. The operator records events with time and date stamps (using synchronized time sources) in the logging system and keeps the information for a defined period of time in central archives.	● OTORIO's RAM^2 ingests logs from multiple systems in the network to provide a single pane of glass for events that are meaningful in the context of OT security. ● RAM^2 also assists in verifying that critical logging capabilities are enabled in the relevant systems as required for compliance with security standards requirements. ● Integrations can be extended to support new types of data sources using a flexible and open plugin-based architecture.
8.3 Correlation and Analysis NIS regulation: Mechanisms for the detection and adequate assessment of incidents by the Correlation and analysis of the recorded log data are to be implemented. For correlation and analysis, the operator uses a system that is safety-related, summarizes and evaluates events to identify incidents. The operator sets up a special information system for correlation, analysis and further processing of incidents. The operator takes this into account when designing Systems in particular the confidentiality of the stored data.	● RAM^2 uses out-of-the-box expert-defined correlated alerts ("Insights") to automatically analyze and detect suspicious patterns. ● RAM^2 ingests data from a wide variety of cross-domain sources using APIs, Syslogs, passive monitoring, active querying and processing of offline files. The events from all sources are automatically mapped to standard types, so the correlation logic can be agnostic to the source of data, and new sources can be added to leverage any vendor system that is available at the operator's network. ● OTORIO's cyber experts are continuously extending the platform's analysis and detection capabilities. ● It is also possible to create new insights according to specific characteristics of the operator's environment.
9. Incident Management	
9.1 Incident Response NIS regulation:	● OTORIO's RAM^2 alerts and insights include prescriptive step-by-step mitigation playbooks for efficient response to detected incidents.

Processes for responding to incidents must be created, maintained and tested. The operator creates and implements processes and procedures to respond to incidents that affect the functioning or security of a network and information system. The operator defines clear roles and responsibilities in this regard. The processes and procedures are regularly updated and checked through tests and exercises. The operator ensures that forensic knowledge and capacities are either available in-house or can be called up as required via a contract with a service provider. The operator ensures that findings and lessons learned from previous incidents flow into its processes and procedures (lessons learned).	● Mitigation steps can be updated and enhanced according to the operational processes of the operator's organization and lessons learned. ● OTORIO’s professional services provide best practices for OT security processes (change management, proactive risk management ,and detection and response). They also work with the operator to define the roles and responsibilities, and tailoring the OT security processes to the operator’s specific organization characteristics.
9.2 Incident Reporting NIS regulation: Processes for responding to incidents must be created, maintained and tested. The operator creates, implements and regularly updates processes and procedures for internal and external reporting of incidents. In addition, the operator develops processes and procedures in order to be informed immediately in the event of incidents at service providers and suppliers, provided that the incidents could be relevant to the security level or situation of the operator.	● RAM^2 enables generation of different reports from asset inventory and vulnerability to compliance and risk assessment. ● The platform includes a mechanism for automatic email notification regarding alerts according to operational processes and severity, sent to predefined distribution lists, even when not reviewing the data within the system. ● RAM^2 is based on an open platform that can also distribute the alerts and insights to other organizational systems through API and Syslog, to streamline OT security into existing flows and processes of the operator’s organization.
9.3 Incident Analysis NIS regulation: Processes for analyzing and evaluating incidents and collecting relevant information must be created, maintained and tested in order to promote the continuous improvement process. The operator establishes processes and implements procedures to enable the analysis and evaluation of detected and/or suspected incidents. Furthermore, the operator defines and tests processes for collecting and evaluating analysis-relevant information.	● RAM^2 enables and structures data collection and analysis processes. ● It supports the collaboration between teams via case management mechanism or by streaming the data into existing systems and flows.
10. Business Continuity	
10.1 Business Continuity Management NIS regulation: The restoration of the provision of the essential service at a previously defined level of quality after a security incident must be guaranteed. The operator defines goals and strategic guidelines for business continuity management in the event of a security incident. The operator is responsible for setting up an efficient emergency and crisis management system for systematic preparation for dealing with security incidents or damaging events, in particular for	● RAM^2 manages assets and related attributes, vulnerabilities and threats within the operational hierarchy context. ● The operator can use the platform to manage impact information at the single asset or process level, to monitor the operational “crown jewels” and use the data for risk quantification. ● The risk data is aggregated so the operator can review it, top-down, from an operational perspective and proactively assess the business and impact and risk and across business units in the operational environment.

restoring the provision of essential services. As a basis for emergency and crisis management, the operator carries out a business impact analysis of its network and information systems and updates it regularly.	
10.2 Emergency Management NIS regulation: Emergency plans are to be drawn up, applied, regularly evaluated and tested. The operator creates an emergency manual and ensures that the emergency processes defined in it are carried out accordingly. The operator ensures that knowledge and lessons learned from previous security incidents flow into the emergency plans. The operator conducts regular emergency drills to check the effectiveness of emergency preparedness measures.	● RAM^2's built-in playbooks provide step-by-step guidance for risk mitigation for each detected incident type that can be followed and implemented by the operator. ● OTORIO's services can provide training to up-skill the operator's teams' response capabilities.
11. Crisis Management	
11.1 Crisis Management NIS regulation: Crisis management framework conditions and processes are to be defined, implemented and tested to maintain essential service before and during a security incident. The operator defines the organization and responsibilities for crisis management in the event of security incidents, creates suitable alarm plans and implements suitable processes and procedures for crisis management. The operator ensures that crisis management activities are coordinated with internal and external partners (e.g. internet service providers, CERT, authorities, system integrators, etc.).	NA