infosync

INTEGRATED RISK MANAGEMENT PLATFORM

esc2 security

esc2
security

ESC 2 Srl

Roma Via C. Colombo,112 - 00147
Milano Via Fabio Filzi, 5 - 20124

info@esc2.it

T +39 06 5107931

F +39 06 510793506

www.esc2.it

twitter.com/ ESC2_Security
linkedin.com/ESC2 Security

THE CONTEXT

Data protection from threats that compromise its authenticity, integrity, confidentiality and availability is the fundamental objective of every organization that manages assets and information, as well as an integral part of the National Cybernetic Protection and IT Security Plan, because the information constitutes an intrinsic value to the organization, public or private.

The strategic objective of every organization is to evolve the processes of Security Governance through an approach based on the analysis and management of the main risk scenarios that affect the confidentiality, availability and integrity of information, as well as typical risk scenarios of National Critical Infrastructures and of actors of strategic importance for the Country system.

The adoption of an integrated process of Information Security and Privacy Governance based on risk, in addition to being a basic principle of the most recent national and international provisions, rules and standards regarding privacy and IT security.

With the rapid evolution of information and communication technologies, information systems have assumed a central importance in the organizational and functional structure of all the companies.

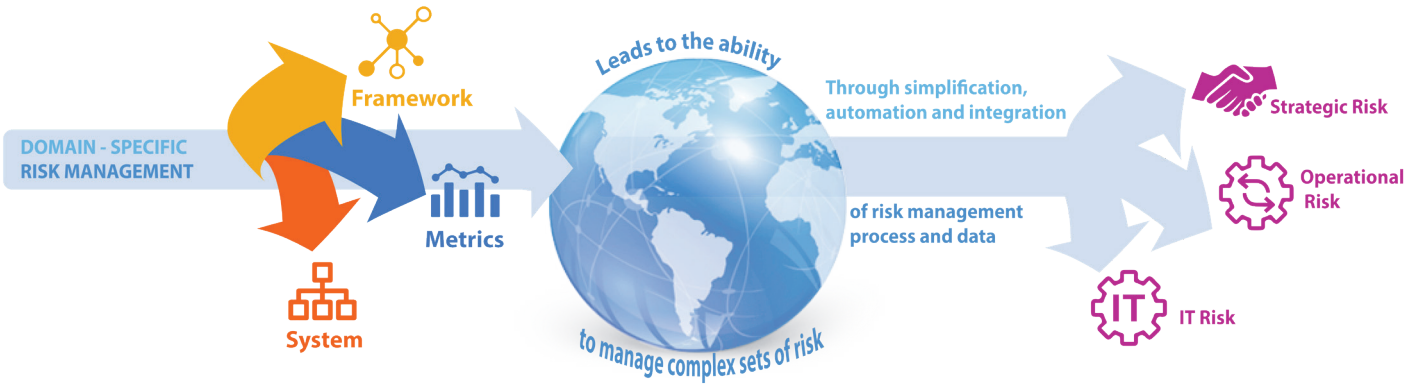
In this operating context, characterized by continuous changes in technologies and the spread of increasingly high digital content business processes, the failure to safeguard the security of IT and non-IT resources translates into potentially significant direct and indirect impacts on the strategic objectives of each organization, as well as on the economic-asset values.

INDICE

The spread of digital technologies based on the "Internet" paradigm, such as Cloud Computing, as well as the use of service models in Outsourcing, have favored the redesign of the organizational boundaries of companies, more open and connected with other subjects and with their customers, creating on one hand new business opportunities, but on the other hand realizing new types of risk scenarios to manage.

An integrated risk-based approach enables the economic-financial planning processes to be supported to implement the technical and organizational measures necessary to mitigate them, both for information and material and instrumental components, as well as for the protection of personnel safety (of the organization and of the employees / customers / suppliers fleet), also through the definition of adequate metrics for the assessment of the potential direct and indirect impact of events that have occurred or potential (detect, remediation, image damage , loss of credibility / reliability / competitiveness, costs of inefficiencies, possible loss of life, etc.).

With this in mind and with the aim of supporting integrated risk governance, ESC 2 designed and implemented the Infosync platform, an Integrated Risk Management solution, based on recognized guidelines, standards and best practices, such as: ITIL, COBIT 5, ISO27000 Family, NIST Cybersecurity Framework.



GARTNER MENTION

Infosync is the only solution in Europe to be mentioned in the Gartner report "Critical Capabilities for IT Risk Management Solutions - August 2018" among the main IT Risk Management solutions vendors.

“The inclusion of INFOSYNC in the Gartner 2018 report on ITRM Critical Capabilities, in continuity with the Notable Mention received in the 2017 Magic Quadrant for IT RM, is an important recognition of the Infosync solution growth path for IT Risk Management in these years, and rewards constant attention to market and regulatory developments, and to the functional needs of customers by the ESC 2 team.

In particular, as described in the Gartner report, we have made the Cloud version available with fee in SaaS for customers who prefer activation agility and a model with OPEX costs including maintenance to purchase a perpetual license and annual maintenance, and that they do not need the “On Premises” solution. We have also released the advanced reporting module based on Tableau with many templates immediately available and customizable, making the entire strategic reporting cycle much faster and more responsive to our customers’ needs. I believe there is a large market space for the INFOSYNC solution both in Italy, the country where we are the only vendor that has its head office, and in Europe.”

The comment of Ing. Claudio Ragno, after the publication of the report on August 20, 2018.

Description of the solution

Infosync

Infosync is the Integrated Risk Management (IRM) platform to support the management of the various Information Security and Privacy Risk Management activities, including the analysis of threats and vulnerabilities, technological and non-resource risk analysis IT (in terms of applications, infrastructures and networks) and the risks associated with third parties involved in the process (eg vendors, service providers, etc.).

Objectives and benefits

The Infosync platform aims to define a governance model of operational risks related to the management of ICT (Information and Communication Technology) resources in the production cycle of the value of an organization. The Infosync platform has been developed according to the following principles:

- **Holistic and integrated view of risk,** built through the cohesion and measurement of different types of scenarios, concerning the change, evolution, operation of the ICT infrastructure and services, as well as concerning the incident, problem and security methods management;
- **Unified reporting** to supervisory bodies and top management, regarding the state of IT risk in relation to the state of IT resources as well as the methods and practices adopted to provide the services offered;
- **Focus on risk in decision-making processes,** aimed at making the technological and service infrastructure evolve in a sustainable manner consistent with the objectives of the stakeholders;
- **Monitoring and optimization of the risks** assumed for the sustainable achievement of the defined objectives;
- **Adherence to international standards** and best practices.

Specifically, the Infosync workflow integrates IT risk scenarios (management and life cycle of the technological infrastructure - Service Portfolio Management, Design, Development, Test and Rollout, Operations) with those of Information and Operational Security, as well as with scenarios of risk concerning the processing of personal data.

Technological risk assessments are also subject to the internal control and monitoring model, implemented through control plans, Business Impact Analysis and Business Continuity processes as well as the analysis and management of historical and potential incidents.

The benefits of the Infosync platform can be summarized as follows:

SUMMARY AND REPRESENTATION OF PERFORMANCE AND IT AND SECURITY RISK

- Automatic collection and processing of information, according to defined integration patterns and models.
- Integrated, flexible and configurable IT risk management processes.
- Evidence of the most critical areas in order to identify the best management and treatment options.

CENTRALIZATION OF DECISION-MAKING AND REMEDIATION PLANS

Support to strategy and planning, reducing the efforts, time and resources used to improve performance and IT security levels.

MONITORING THE EFFECTIVENESS OF THE IMPLEMENTED SOLUTIONS

- Monitoring of the state of IT security through Security Key Performance Indicators and Key Risk Indicators.
- Customizable metrics that can be managed independently through the user interface.
- Automatic and schedulable alerting and communication processes.

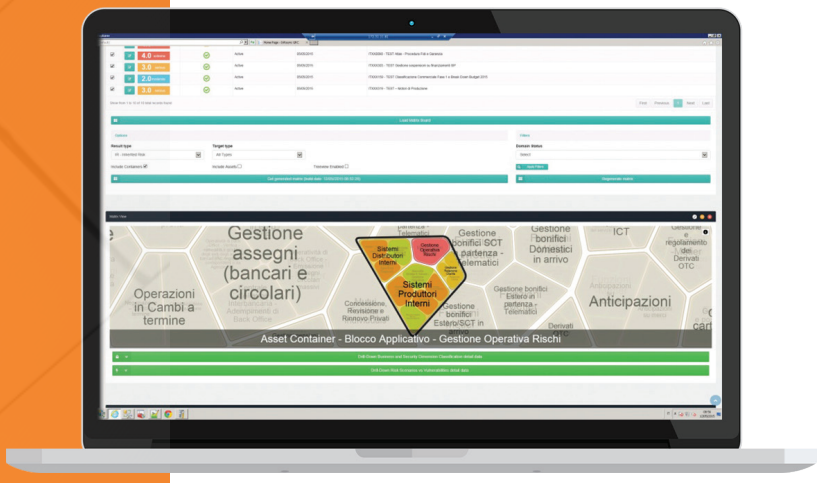
INFORMATION SHARING

- Profiled sharing of information, inside and outside the organization.
- Management and control of access to dashboards and visibility of information within dashboards, through profiling functions of visibility and integration with access management systems.

Features e Capabilities

Infosync is based on the following paradigms:

- *Modular functional organization that allows a plan to activate progressive functions in the medium term, able to follow the evolutionary roadmap of the Integrated Risk Management framework;*
- *flexible architecture able to support the processes of integration with the systems and solutions (current and future) of Cybersecurity, IT and Network Operation, as well as with other data sources such as the administration or third party entities involved in the process;*
- *solid and flexible data model, able to normalize the information produced or collected by the different Cybersecurity and IT Operation processes;*
- *IT and Cyber Risk Management workflow that allows the management of the various security assessment activities (internal and external) and risk management, according to a model based on the identification and control of activities;*
- *data-analytics engine capable of allowing a visual analysis of information in defined reporting models (eg Key Performance Indicator, Key Risk Indicator) and provides functions that help define structures that can be easily customized based on changing strategic and operational needs.*

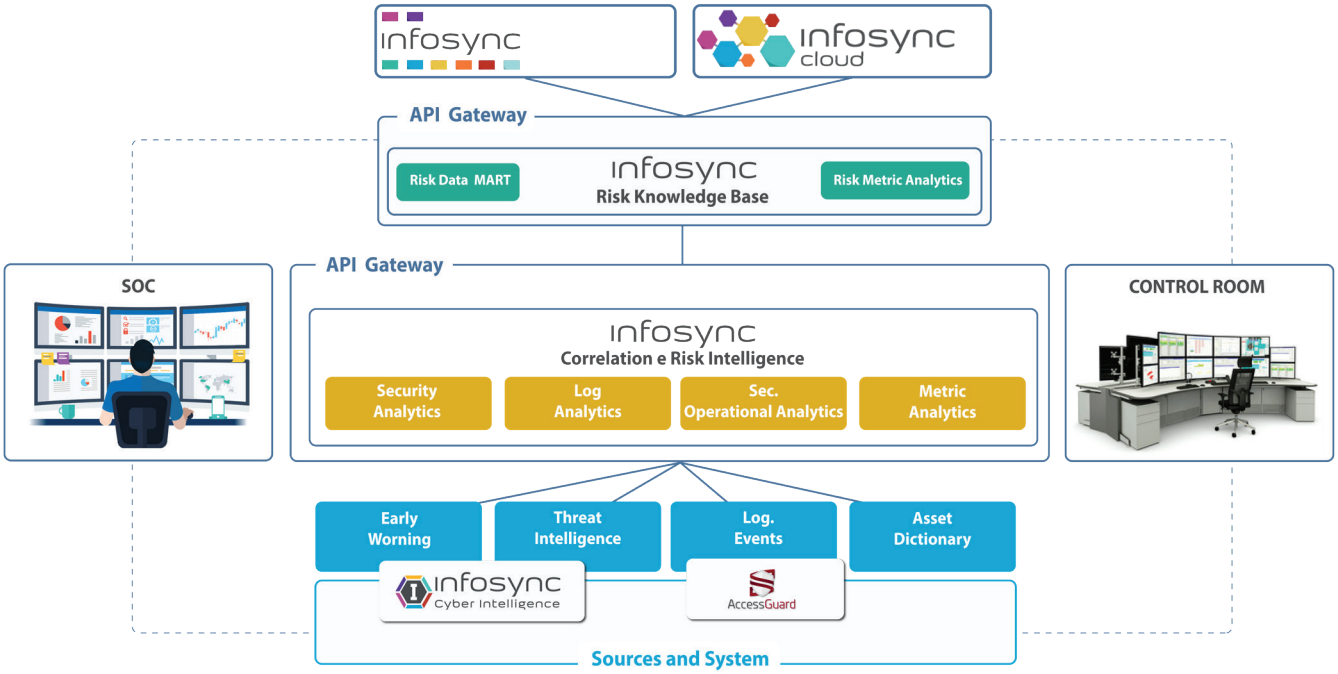


Infosync is able to support integrations with the most common Cyber-Risk Management systems, such as:

- CMDB (Application Security Testing, Secure Configuration Management),
- TVM (Threat and Vulnerability Management),
- TIP (Threat Intelligence Platforms),
- IAM (Identity and Access Management) through Active Directory (AD), LDAP, or other services.

Furthermore the application supports RBAC (role-based access controls) processes to functions and contents.

The solution guarantees integration with SIEM (Security Information Event Management), SOAR (Security Orchestration, Automation and Response), UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention) systems.



The solution, through the integrations described, enables the risk analysis and identification processes in automatic and "near real time" mode, according to a continuous evaluation approach of the effectiveness of the controls, of the compliance, and of the residual risk for each asset or process.

These processes are supported by a model of representation of the Enterprise Architecture (representation of the structure of an organization, its operational processes, supporting information systems, information flows, technologies used, geographical locations) that allows, where possible , to manage the relationships between IT assets, at different levels, with the processes of management and processing of information, or organizational resources and processes of the organization.

Infosync has pre-configured workflow templates to facilitate risk assessment processes, control assessments and audits (internal and external), as well as communication between the various IT, Security and Privacy compliance representatives.
The solution allows you to map internal controls or policies with respect to libraries of specific requirements referable to frameworks, standards and best practices related to IT contexts, cyber, privacy and business continuity, available out-of-the-box or easily configurable to system.

Infosync enables qualitative and quantitative risk assessment processes. The risks can be linked to the organization's high-level processes and functions, through a process of modeling threats and vulnerabilities with respect to risk assessment processes for specific and different contexts.

The solution has risk mitigation processes supported by action definition processes (owners, expiration, manager, necessary budget, priorities) and through automatic models for defining the implementation priorities of the actions (eg Compliance, Mitigation levels, capacity security solutions to mitigate risk, etc.), or through the integration of project management tools in use or usable by the administration.

The Infosync Modules

AM **Asset Management** - Basic module of the platform, which allows the cataloging and management of information (inventory) relating to Assets, Asset Containers and Processes - Strategic Processes (Competitive or innovation and transformation), Operating Processes and Support Processes. It allows integration with third-party asset management systems aimed at enhancing the security and business impact dimensions. Enabling Asset Experience processes (Asset-centric Vision of risk and Event Analysis processes) and Enterprise Architecture management, which also guarantees a mapping of information flows between the various assets (mapping of the relationships between the objects cataloged in the AM module).

RM **Risk Management** - Risk Management processes management module, through a process based on periodic assessment activities (context or domain), characterized by:

- definition of the assessment library (eg 27001, PSD2, NIST, etc.) and of compliance perimeters specific to each context;
- definition of the perimeter (set of Assets);
- definition of the roles participating in the assessment;
- management of operational and cyclical phases of Risk Management (risk identification, risk analysis and risk evaluation), What-If Analysis, Action Plan and Monitoring.

DP **Data Protection (GDPR)** - Data Protection Process Management Module aimed at supporting compliance with the new European GDPR - General Data Protection Regulation and integration with the Risk Management processes of the platform.

GA **Gap Analysis e Audit** - Module for the management of the Gap-Analysis and Compliance Assessment processes as well as the Audit programs (Internal Audit and Third-Party Audit and Suppliers), also through web-portal for self-assessment execution by the interested third parties.

CE **Collector Engine -** Module for the management of integration processes with external data sources. The module allows to define and schedule Collection processes and to carry out the transformation and normalization processes necessary for integration.

SA **Security Analytics** - Data Analytics Module, for Dashboarding, Monitoring, Insight and Discovery processes of data integrated in the proprietary data model (Risk Hub), to support top Management and Operational Reporting.

EW **Early Warning** - Functions to support the process of proactive management of vulnerabilities and security threats, through automated correlation processes of information related to the impacted assets with the feeds published by NIST (National Institute for Standard and Technologies) and indicators of compromise, designed to offer a solution based on open-source solutions and able to integrate solutions of market Vulnerability Assessment (eg Tenable, Qualys, etc).

esc2
security

elisian group