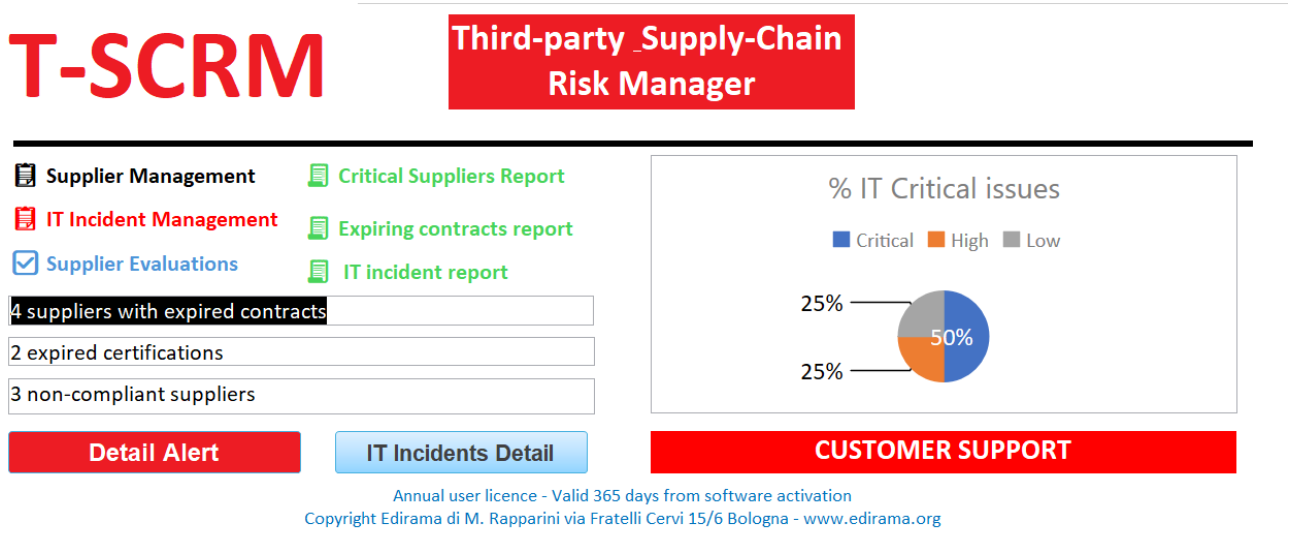


🔐 **Protect your business from Third-Party Supply Chain**

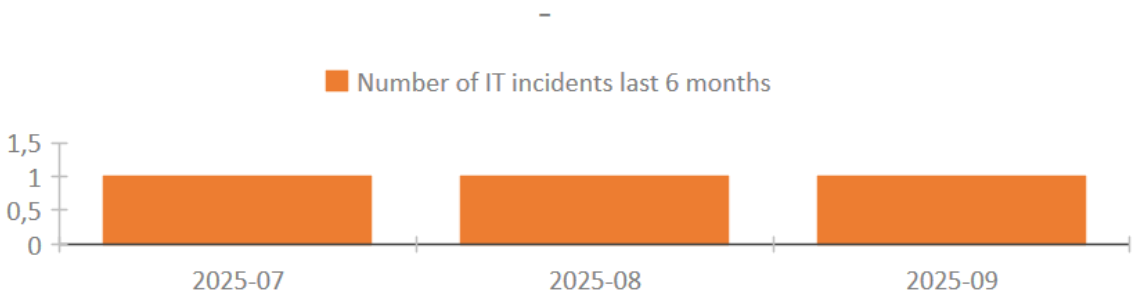
T-SCRM is the professional software designed to identify, assess and monitor cyber risks associated with the supply chain, in compliance with the European NIS 2 Directive **, EU Dora Regulation, ISO 27001** and with good governance and security practices.

With an intuitive dashboard, pre-configured assessment tools and automatic alerts on critical issues and deadlines, T-SCRMis the ideal tool for companies, consultants who want to move from Excel sheets to structured **and professional** supplier risk management.

Summary of Supplier Incidents

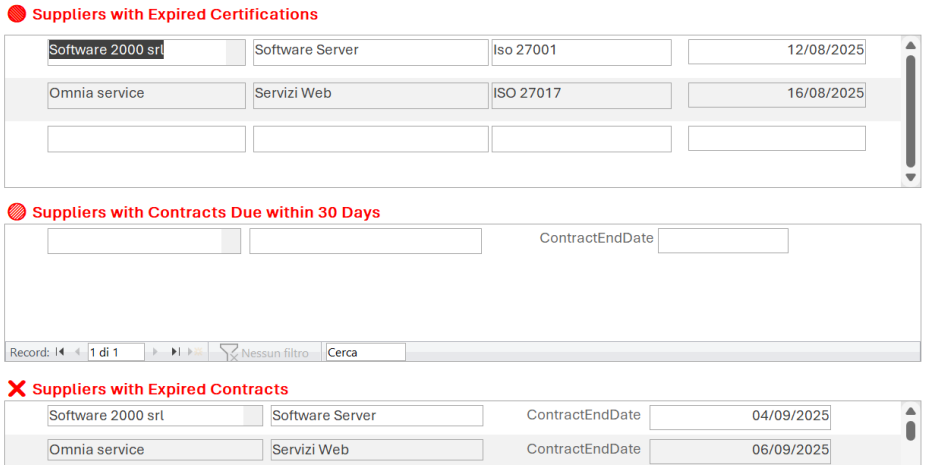
Accident for supplier

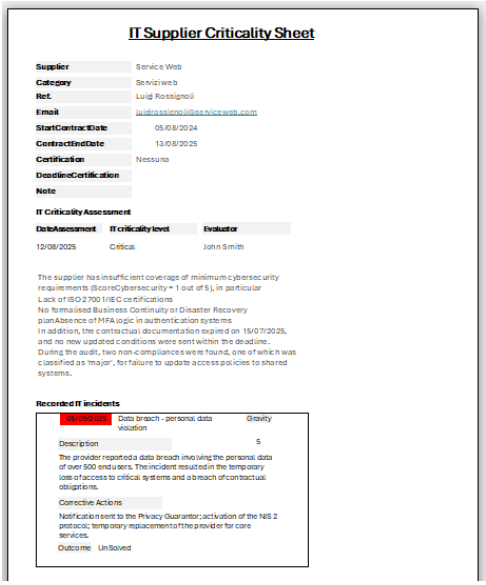
Supplier	Total Acciden	Medium Severity
Omnia service	2	4
Privacy and Policy srl	0	
Service Web	1	5
Software 2000 srl	0	



Key features

- Supplier master data
- Automatic IT risk assessment (compliance, cybersecurity, reliability)
- Synthetic indicators and customizable scores
- Monitoring expiring contracts and certifications
- Incident and non-compliance log
- Dashboards with visual alerts and summary graphs
- Audit-ready reporting, NIS 2, DORA, ISO 27001 documentation
- Annual license system with serial code activation




IT Supplier Criticality Sheet

Supplier Service Web
Category Servizi web
Ref. Luigi Rossignoli
Email luigirossignoli@serviceweb.com
StartContractDate 05/08/2024
ContractEndDate 13/08/2025
Certification Nessuna
DeadlineCertification
Note

IT Criticality Assessment

DateAssessment	IT criticality level	Evaluator
12/08/2025	Critical	John Smith

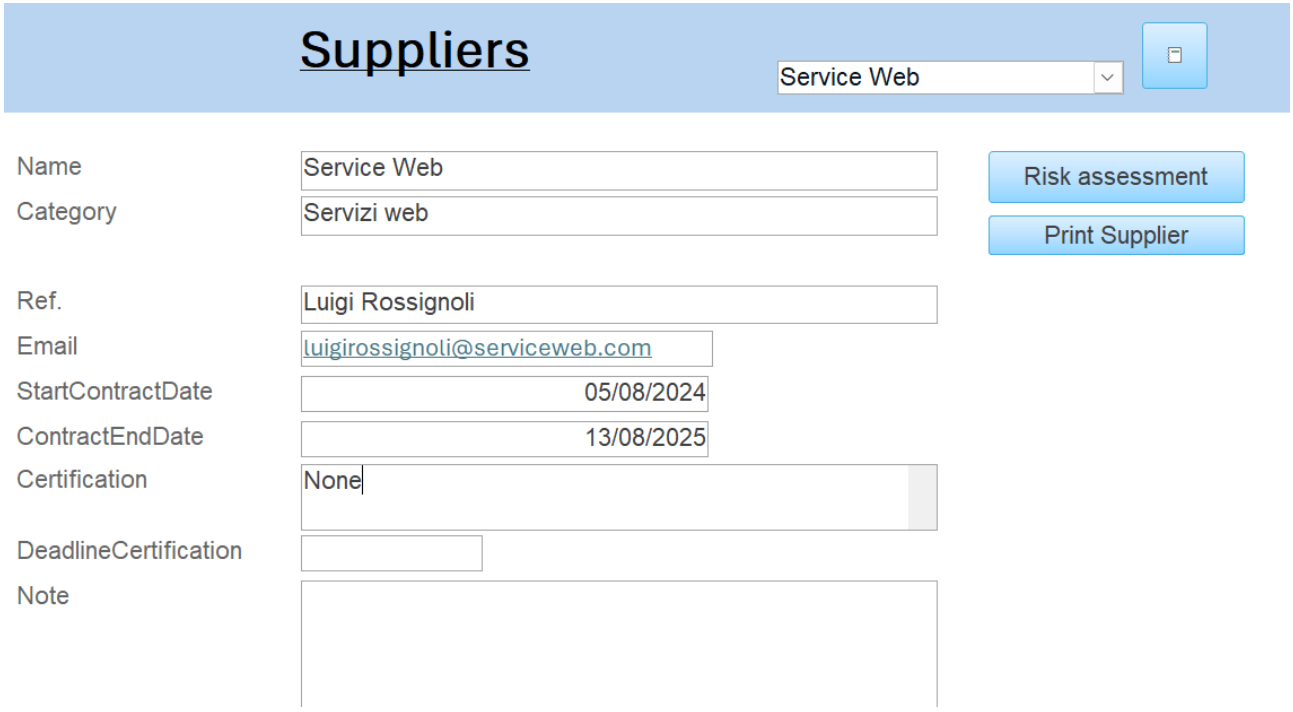
The supplier has insufficient coverage of minimum cybersecurity requirements (ScoreCybersecurity = 1 out of 5), in particular
Lack of ISO 27001/IEC certifications
No formalised Business Continuity or Disaster Recovery plan
Absence of MFA logic in authentication systems
In addition, the contractual documentation expired on 15/07/2025, and no new updated conditions were sent within the deadline.
During the audit, two non-compliances were found, one of which was classified as 'major', for failure to update access policies to shared systems.

Recorded IT incidents

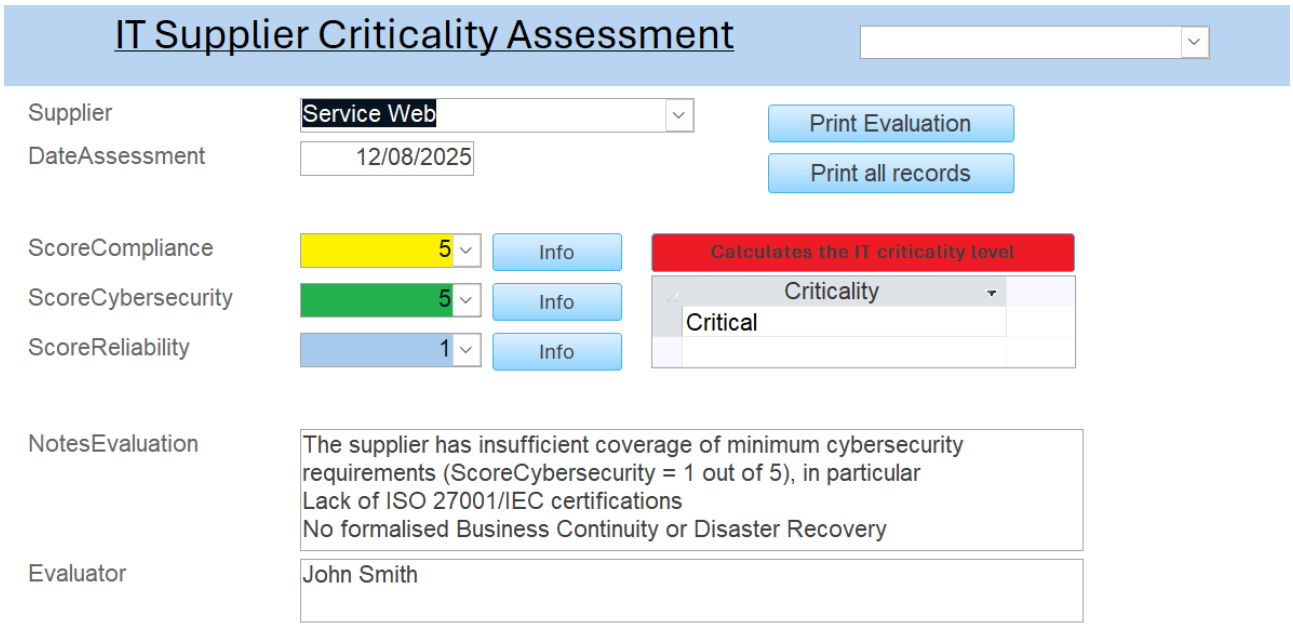
05/09/2025	Data breach - personal data violation	Gravity
Description		5

The provider reported a data breach involving the personal data of over 500 end users. The incident resulted in the temporary loss of access to critical systems and a breach of contractual obligations.
Corrective Actions
Notification sent to the Privacy Guarantor; activation of the NIS 2 protocol; temporary replacement of the provider for core services.
Outcome UnSolved

1) SUPPLIER MANAGEMENT

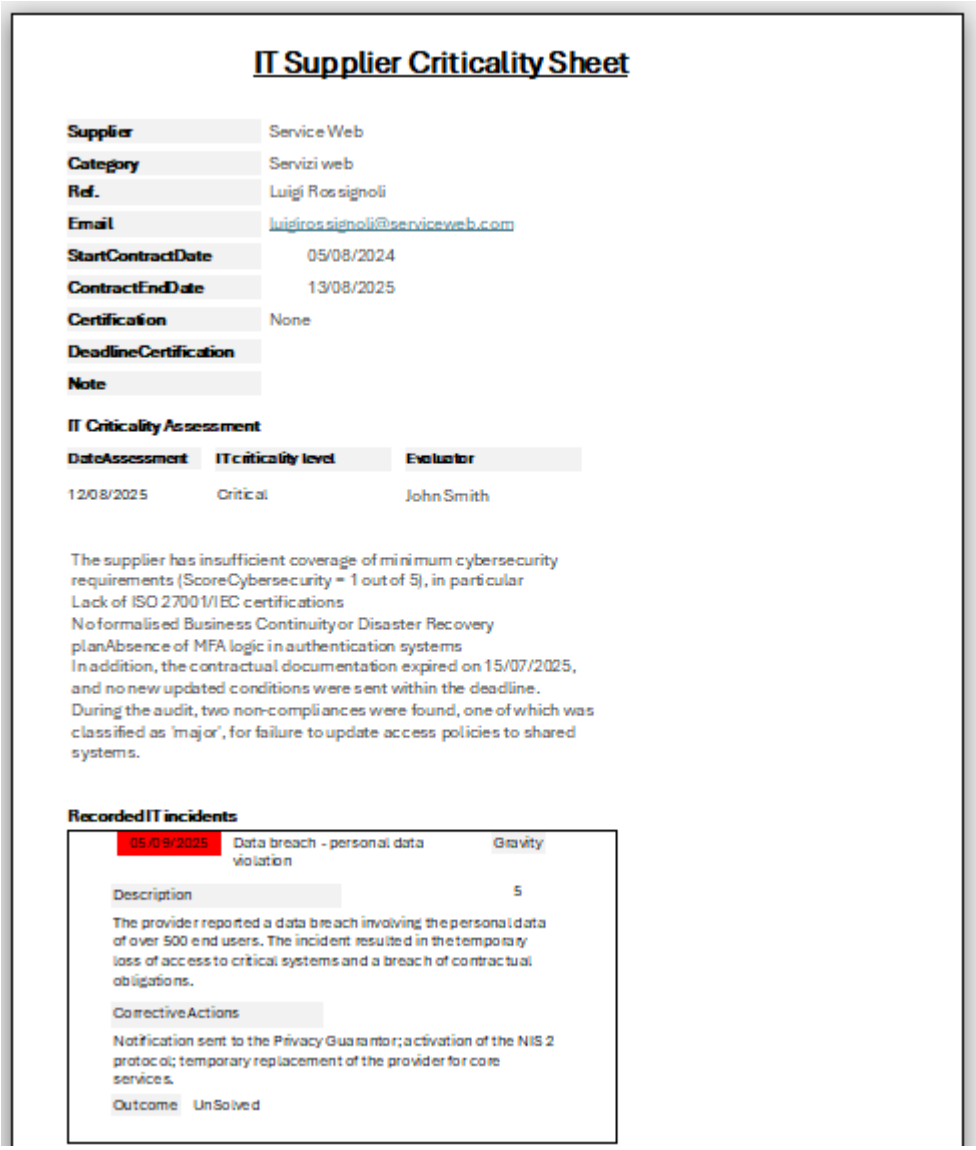


2) SUPPLIER IT CRITICALITY ASSESSMENT



This section allows you to calculate the supplier's IT criticality level automatically.
The evaluation is made by considering three parameters:_ Compliance_ Cybersecurity_ Reliability with a scale of 1 to 5. The software for each parameter provides a detailed scale that can be consulted by the user from the INFO button The software automatically calculates the supplier's IT criticality level and allows you to print the supplier's detailed report with the

relative IT criticality assessment.



IT Supplier Criticality Sheet

Supplier	Service Web
Category	Servizi web
Ref.	Luigi Rossignoli
Email	luigirossignoli@serviceweb.com
StartContractDate	05/08/2024
ContractEndDate	13/08/2025
Certification	None
DeadlineCertification	
Note	

IT Criticality Assessment

DateAssessment	IT criticality level	Evaluator
12/08/2025	Critical	John Smith

The supplier has insufficient coverage of minimum cybersecurity requirements (ScoreCybersecurity = 1 out of 5), in particular
Lack of ISO 27001/IEC certifications
No formalised Business Continuity or Disaster Recovery planAbsence of MFA logic in authentication systems
In addition, the contractual documentation expired on 15/07/2025, and no new updated conditions were sent within the deadline.
During the audit, two non-compliances were found, one of which was classified as 'major', for failure to update access policies to shared systems.

Recorded IT incidents

05/09/2025	Data breach - personal data violation	Gravity
Description		5

The provider reported a data breach involving the personal data of over 500 end users. The incident resulted in the temporary loss of access to critical systems and a breach of contractual obligations.

Corrective Actions

Notification sent to the Privacy Guarantor; activation of the NIS 2 protocol; temporary replacement of the provider for core services.

Outcome UnSolved

Automatically, the software allows from the main Dashboard to highlight:

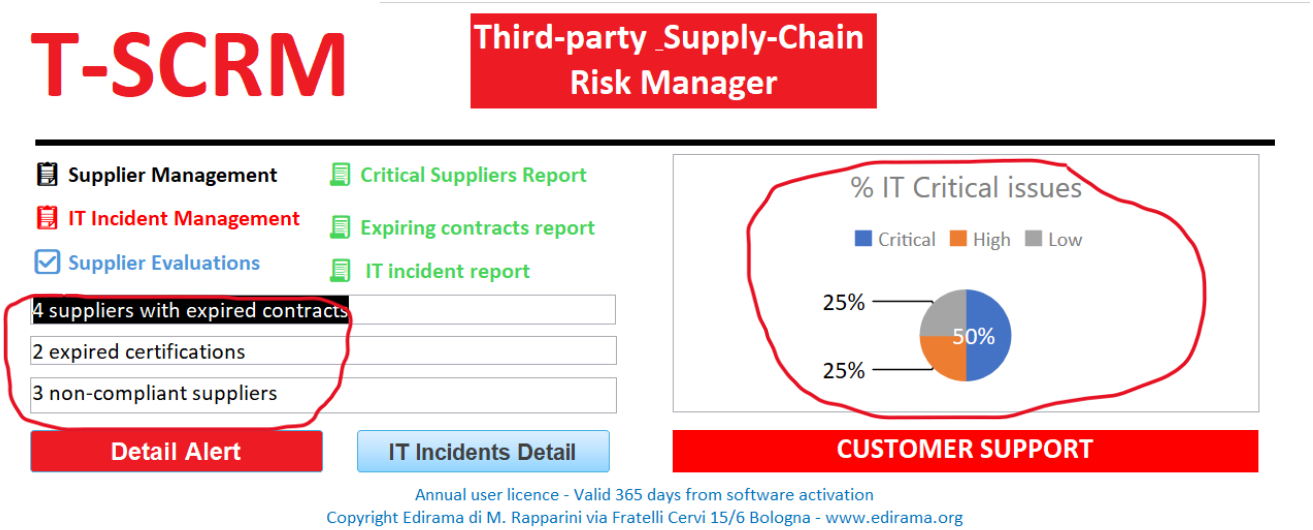
_ critical suppliers

_ suppliers with contracts expiring within 30 giorni

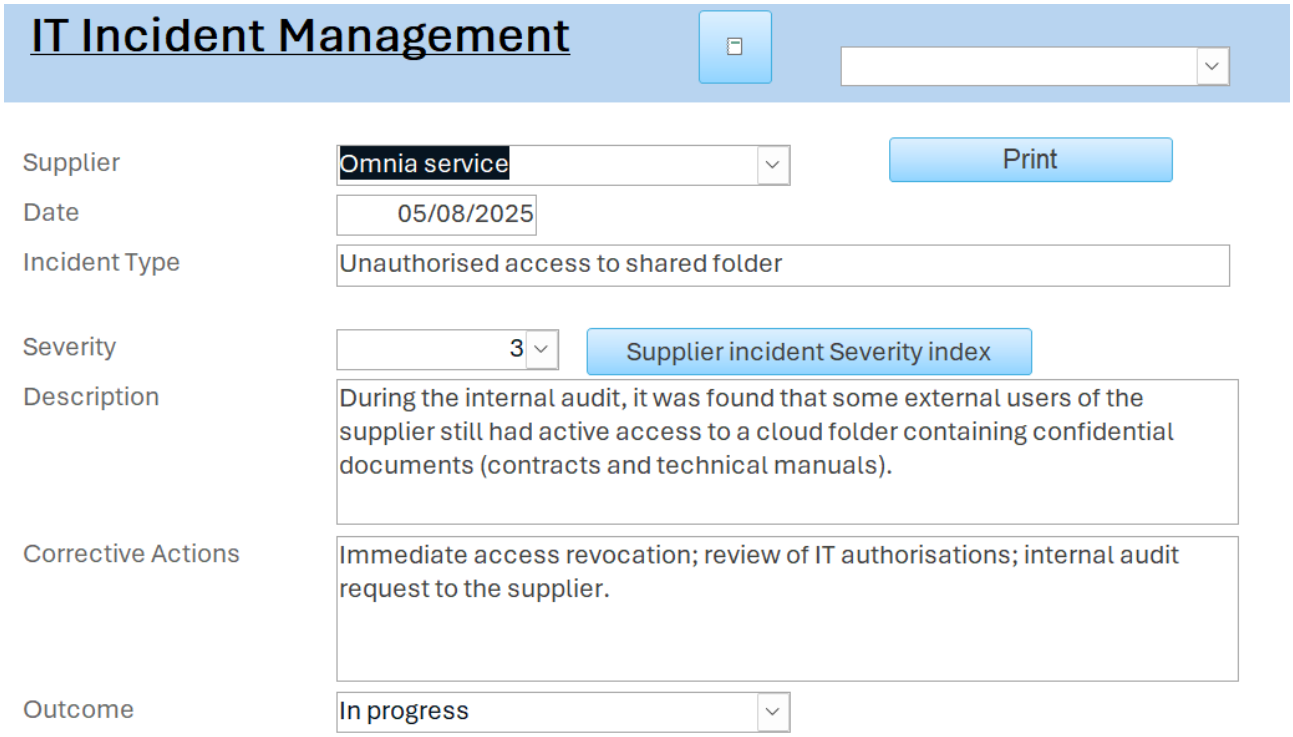
_ suppliers with certification scadute

_ suppliers with expired contracts

and provides an immediate overview of this information as highlighted in the image



3) IT Incident Management allows each supplier to Record, evaluate and archive individual IT incidents, attributing a severity index from 1 to 5 to each individual event, using the evaluation scale that can be consulted by the user. Each IT incident is managed analytically, and tracked for the duration of its assessment.



The software provides two printouts: a general printout and a specific printout for each IT incident, as highlighted in the two images below

Report IT Incidents

Supplier Name	Date	Incident Type	Severity	Description	Corrective Actions	Outcome
Omnia service	15/07/2025	Delayed delivery of documentation	5	The supplier submitted the updated declaration of conformity for the services provided two days late, compared to the contractually established deadline.	Automatic reminder set in the document management system.	Solved
	05/08/2025	Unauthorised access to shared folder	3	During the internal audit, it was found that some external users of the supplier still had active access to a cloud folder containing confidential documents (contracts and technical manuals).	Immediate access revocation; review of IT authorisations; internal audit request to the supplier.	In progress
Service Web	05/09/2025	Data breach - personal data violation	5	The provider reported a data breach involving the personal data of over 500 end users. The incident resulted in the temporary loss of access to critical systems and a breach of contractual obligations.	Notification sent to the Privacy Guarantor; activation of the NIS 2 protocol; temporary replacement of the provider for core services.	UnSolved

Recorded IT incidents

15/07/2025 Delayed delivery of documentation — Gravity 5

Description

The supplier submitted the updated declaration of conformity for the services provided two days late, compared to the contractually established deadline.

Corrective Actions

Automatic reminder set in the document management system.

Outcome Solved

05/08/2025 Unauthorised access to shared folder — Gravity 3

Description

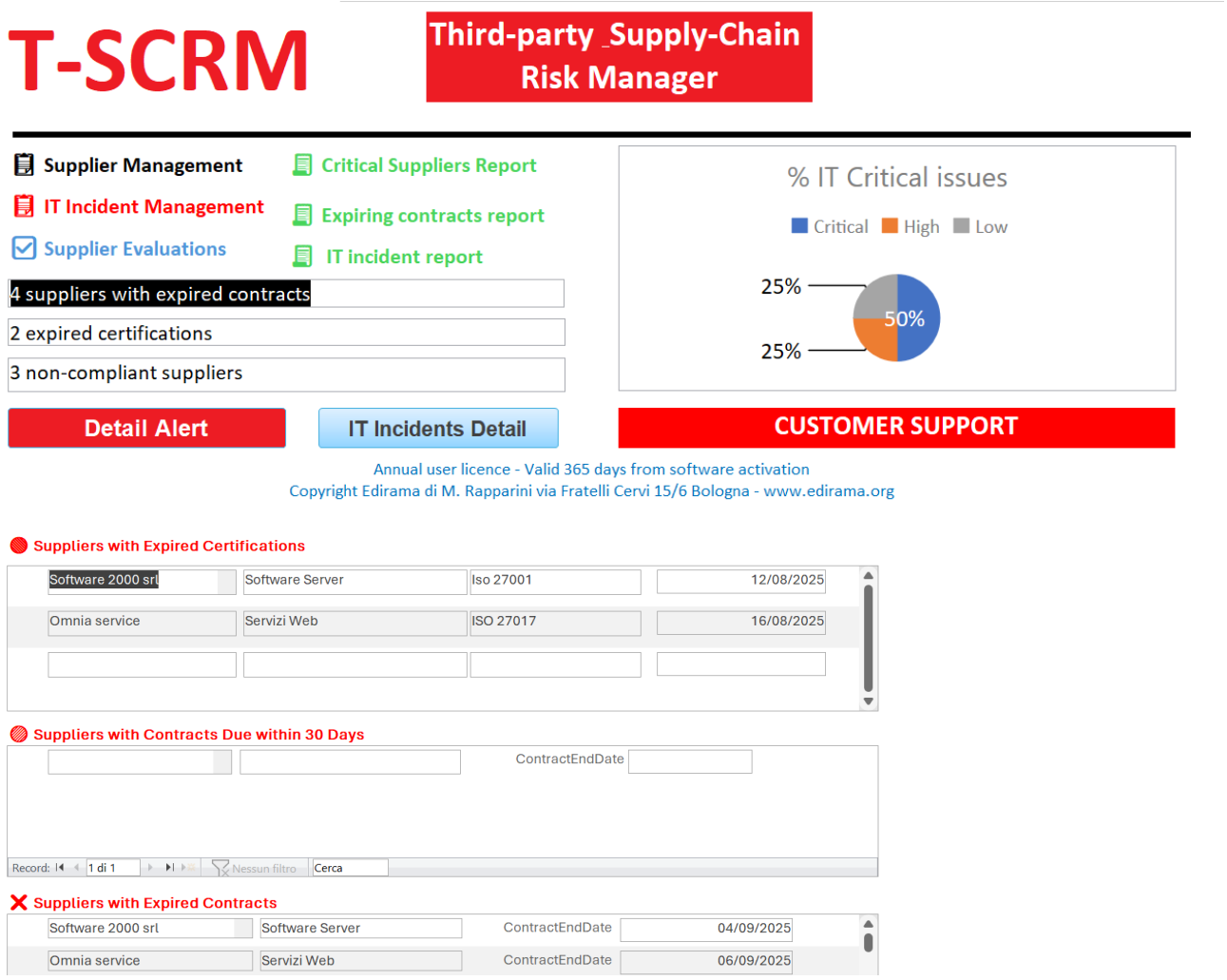
During the internal audit, it was found that some external users of the supplier still had active access to a cloud folder containing confidential documents (contracts and technical manuals).

Corrective Actions

Immediate access revocation; review of IT authorisations; internal audit request to the supplier.

Outcome In progress

4) Dashboards with visual alerts and summary graphs T-SCRM software allows the user to always have the IT criticalities of suppliers and third parties in the foreground, thanks to the 3 Dashboards with visual alerts and summary graphs

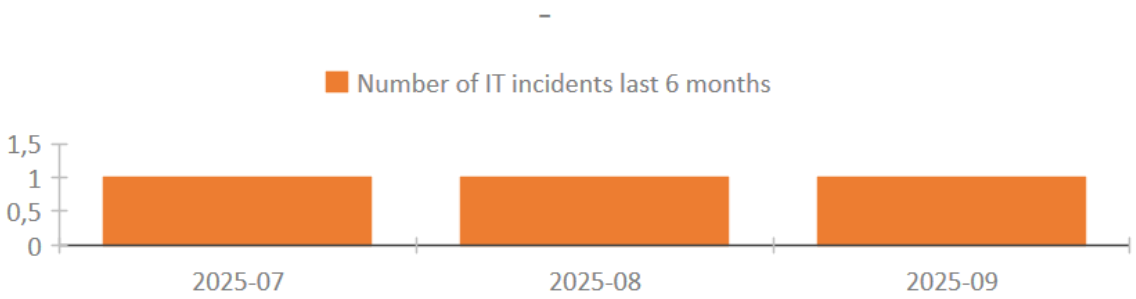


by clicking on the name of the supplier you can directly access the relevant Detail Sheet

Summary of Supplier Incidents

Accident for supplier

Supplier	Total Acciden	Medium Severity
Omnia service	2	4
Privacy and Policy srl	0	
Service Web	1	5
Software 2000 srl	0	



Who is it for?

- NIS 2 consultants, DORA DPOs and cybersecurity experts
- IT, Compliance & Procurement Managers
- Companies subject to NIS 2, DORA or ISO 27001 obligations

Technical requirements

- Operating System: Windows 10/11 or higher

Info

- www.edirama.eu – info@edirama.org