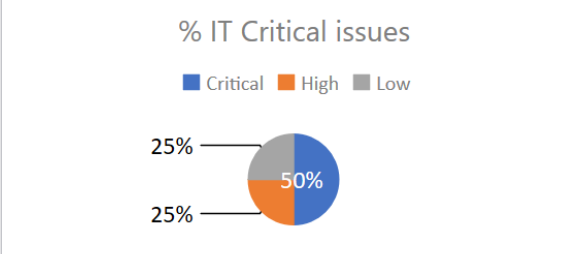


# T-SCRM

## Third-party Supply-Chain Risk Manager

- Supplier Management
  - Critical Suppliers Report
  - IT Incident Management
  - Expiring contracts report
  - Supplier Evaluations
  - IT incident report
- 4 suppliers with expired contracts
- 2 expired certifications
- 3 non-compliant suppliers



**Detail Alert**

**IT Incidents Detail**

**CUSTOMER SUPPORT**

Annual user licence - Valid 365 days from software activation  
Copyright Edirama di M. Rapparini via Fratelli Cervi 15/6 Bologna - www.edirama.org

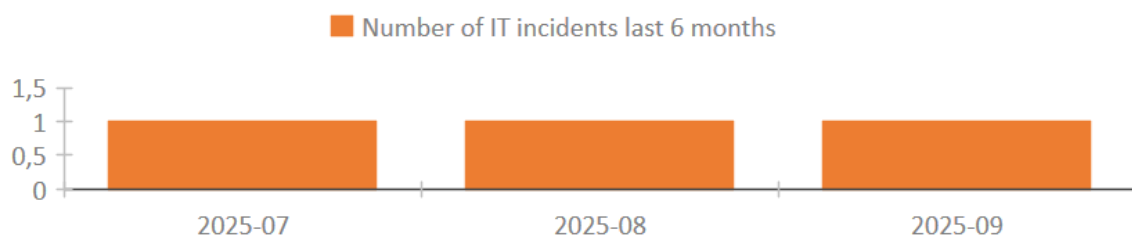
### Protect your business from Third-Party Supply Chain

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-SCRM is 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 Accident	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

● Suppliers with Expired Certifications

Software 2000 srl	Software Server	Iso 27001	12/08/2025
Omnia service	Servizi Web	ISO 27017	16/08/2025

● Suppliers with Contracts Due within 30 Days

		ContractEndDate	
Record: 1 di 1			
Nessun filtro Cerca			

✗ Suppliers with Expired Contracts

Software 2000 srl	Software Server	ContractEndDate	04/09/2025
Omnia service	Servizi Web	ContractEndDate	06/09/2025

**IT Supplier Criticality Sheet**

**Supplier:** Servizi Web  
**Category:** Servizi Web  
**Ref:** Luigi Rostagno  
**Email:** [luigi@scrm@serviziweb.com](mailto:luigi@scrm@serviziweb.com)  
**StartContractDate:** 05/09/2024  
**ContractEndDate:** 13/09/2025  
**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 (Score Cybersecurity = 1 out of 5), in particular Lack of ISO 27001/IEC certifications  
 No formalised Business Continuity or Disaster Recovery plans  
 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**

Description	Severity
Data breach - personal data violation	Critical

**Description:** 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:** Unresolved

## 1) SUPPLIER MANAGEMENT

### Suppliers

Service Web v 📄

Name	<input type="text" value="Service Web"/>	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border: 1px solid #007bff;">Risk assessment</a>
Category	<input type="text" value="Servizi web"/>	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border: 1px solid #007bff;">Print Supplier</a>
Ref.	<input type="text" value="Luigi Rossignoli"/>	
Email	<input type="text" value="luigirossignoli@serviceweb.com"/>	
StartContractDate	<input type="text" value="05/08/2024"/>	
ContractEndDate	<input type="text" value="13/08/2025"/>	
Certification	<input type="text" value="None"/>	
DeadlineCertification	<input type="text"/>	
Note	<div style="border: 1px solid #d9d9d9; height: 40px;"></div>	

## 2) SUPPLIER IT CRITICALITY ASSESSMENT

### IT Supplier Criticality Assessment

v

Supplier	<input type="text" value="Service Web"/>	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border: 1px solid #007bff;">Print Evaluation</a>				
DateAssessment	<input type="text" value="12/08/2025"/>	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border: 1px solid #007bff;">Print all records</a>				
ScoreCompliance	<span style="background-color: yellow; padding: 2px 5px;">5</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span> <a href="#" style="background-color: #007bff; color: white; padding: 2px 5px; border: 1px solid #007bff;">Info</a>	<div style="background-color: #dc3545; color: white; padding: 5px; font-weight: bold;">Calculates the IT criticality level</div> <table style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <tr> <td style="width: 80%;"><span style="border: 1px solid #d9d9d9; padding: 2px;">Criticality</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span></td> <td style="width: 20%;"></td> </tr> <tr> <td><span style="border: 1px solid #d9d9d9; padding: 2px;">Critical</span></td> <td></td> </tr> </table>	<span style="border: 1px solid #d9d9d9; padding: 2px;">Criticality</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span>		<span style="border: 1px solid #d9d9d9; padding: 2px;">Critical</span>	
<span style="border: 1px solid #d9d9d9; padding: 2px;">Criticality</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span>						
<span style="border: 1px solid #d9d9d9; padding: 2px;">Critical</span>						
ScoreCybersecurity	<span style="background-color: green; padding: 2px 5px;">5</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span> <a href="#" style="background-color: #007bff; color: white; padding: 2px 5px; border: 1px solid #007bff;">Info</a>					
ScoreReliability	<span style="background-color: #17aebc; padding: 2px 5px;">1</span> <span style="border: 1px solid #d9d9d9; padding: 2px;">v</span> <a href="#" style="background-color: #007bff; color: white; padding: 2px 5px; border: 1px solid #007bff;">Info</a>					
NotesEvaluation	<p>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</p>					
Evaluator	<input type="text" value="John Smith"/>					

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

<b>Supplier</b>	Service Web
<b>Category</b>	Servizi web
<b>Ref.</b>	Luigi Rossignoli
<b>Email</b>	<a href="mailto:luigirossignoli@serviceweb.com">luigirossignoli@serviceweb.com</a>
<b>StartContractDate</b>	05/08/2024
<b>ContractEndDate</b>	13/08/2025
<b>Certification</b>	None
<b>DeadlineCertification</b>	
<b>Note</b>	

**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.

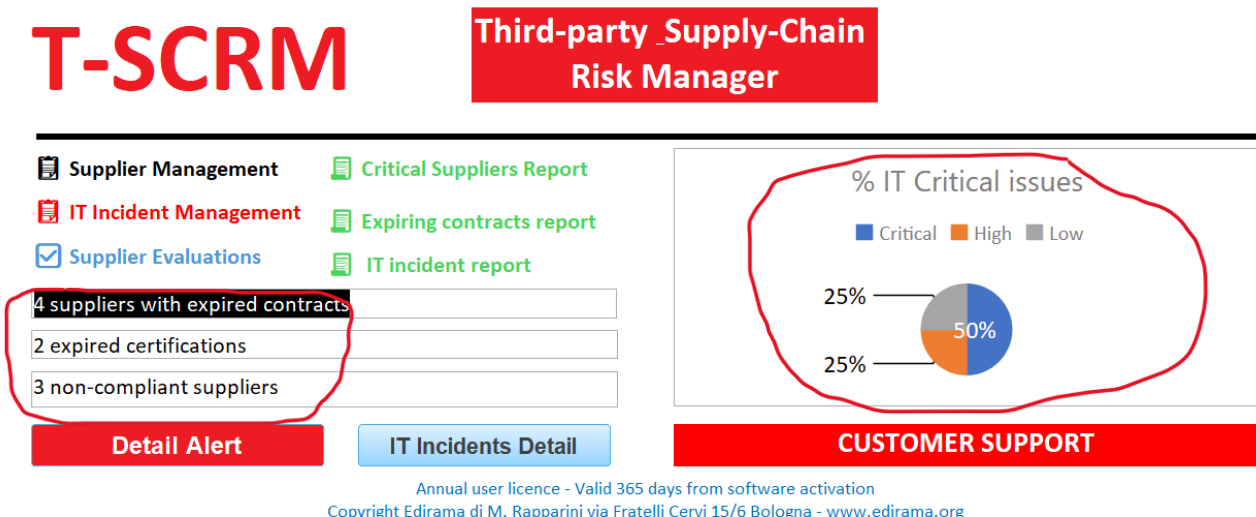
**Recorded IT incidents**

Date	Description	Gravity
05/09/2025	Data breach - personal data violation	5
	<p><b>Description</b></p> <p>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.</p> <p><b>Corrective Actions</b></p> <p>Notification sent to the Privacy Guarantor; activation of the NIS 2 protocol; temporary replacement of the provider for core services.</p> <p><b>Outcome</b> UnSolved</p>	

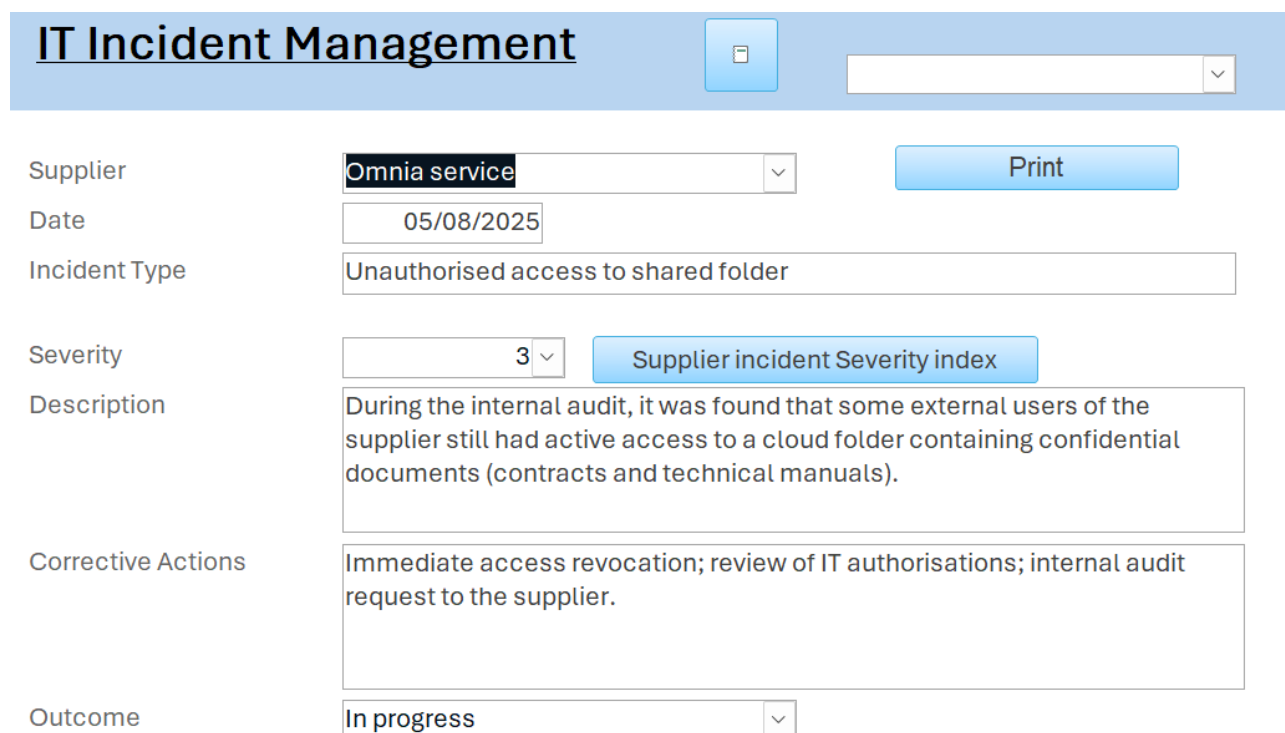
Automatically, the software allows from the main Dashboard to highlight:

- \_ 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 screenshot shows the 'IT Incident Management' interface. At the top, there is a header with the title 'IT Incident Management' and a search bar. Below the header, there is a form with the following fields and values:

Supplier	Omnia service	Print
Date	05/08/2025	
Incident Type	Unauthorised access to shared folder	
Severity	3	Supplier incident Severity index
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	

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.	<b>Solved</b>
	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.	<b>UnSolved</b>

### Recorded IT incidents

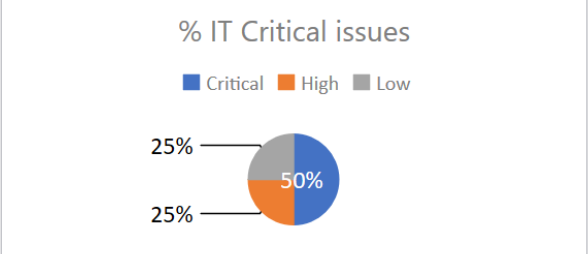
<b>15/07/2025</b>	Delayed delivery of documentation	Gravity
Description		5
The supplier submitted the updated declaration of conformity for the services provided two days late, compared to the contractually established deadline.		
Corrective Actions	Automatic reminder set in the document management system.	
Outcome	Solved	
<b>05/08/2025</b>	Unauthorised access to shared folder	Gravity
Description		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).		
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

# T-SCRM

## Third-party Supply-Chain Risk Manager

- Supplier Management
  - IT Incident Management
  - Supplier Evaluations
  - 4 suppliers with expired contracts
  - 2 expired certifications
  - 3 non-compliant suppliers
- Critical Suppliers Report
  - Expiring contracts report
  - IT incident report



**Detail Alert**

**IT Incidents Detail**

**CUSTOMER SUPPORT**

Annual user licence - Valid 365 days from software activation  
Copyright Edirama di M. Rapparini via Fratelli Cervi 15/6 Bologna - www.edirama.org

### Suppliers with Expired Certifications

Software 2000 srl	Software Server	Iso 27001	12/08/2025
Omnia service	Servizi Web	ISO 27017	16/08/2025

### Suppliers with Contracts Due within 30 Days

		ContractEndDate	
Record: 1 di 1			
Nessun filtro			
Cerca			

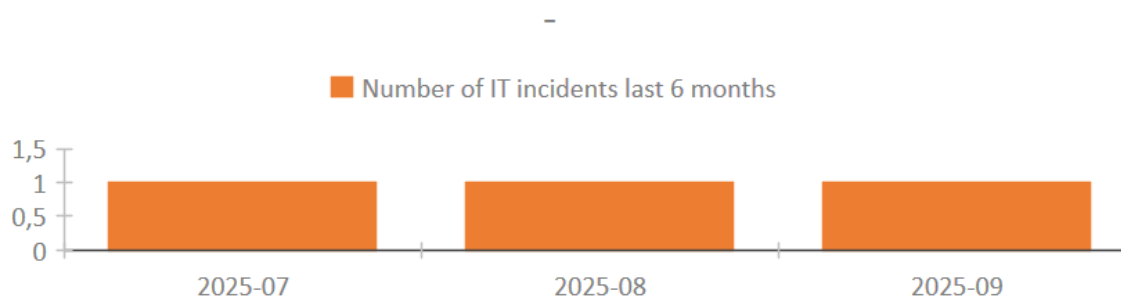
### Suppliers with Expired Contracts

Software 2000 srl	Software Server	ContractEndDate	04/09/2025
Omnia service	Servizi Web	ContractEndDate	06/09/2025

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](http://www.edirama.eu) – [info@edirama.org](mailto:info@edirama.org)