

La Gestione Integrata del Rischio Informatico
Business Impact Analisys

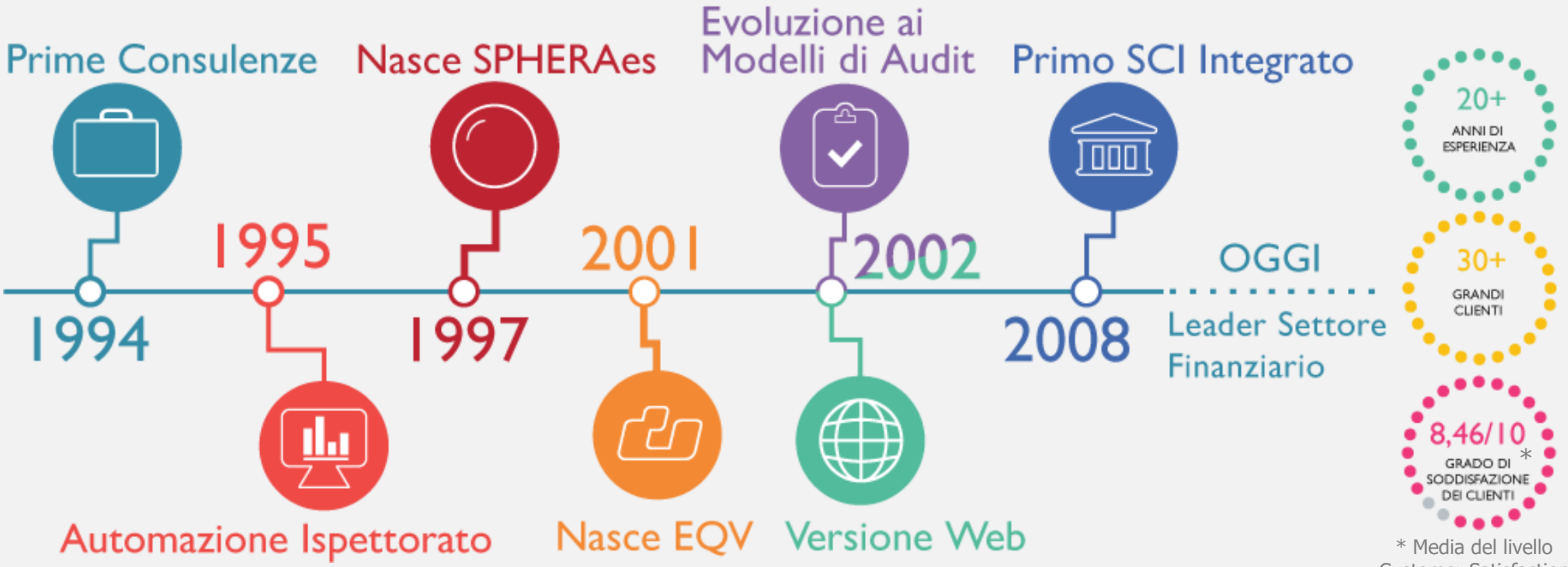
Contesto

Il **18.10.2024** scadranno i termini per adeguarsi alla NIS2, la Direttiva dell'Unione Europea in materia di cybersicurezza (D.E. 2022/2555).
La NIS2 stabilisce un piano di difesa comune contro rischi e minacce informatiche, definendo:

- 🎯 misure di gestione e prevenzione del rischio
- 🎯 obblighi di vigilanza e comunicazione sullo stato di sicurezza dei propri sistemi IT
- 🎯 l'istituzione di un'Autorità nazionale per la gestione delle crisi informatiche

- Trasporti (aerei, ferroviari, marittimi, stradali)
- Banche e infrastrutture del Mercato Finanziario (**DORA** Regolamento (UE) 2022/2554)
- Sanità (**PNRR**)
- Acque potabili e reflue
- Mercati online
- Motori di ricerca, piattaforme di servizi di social networking
- Gestione servizi ICT (B2B)
- Pubblica Amministrazione
- Gestione rifiuti
- Produzione e distribuzione di prodotti chimici
- Produzione, trasformazione e distribuzione di alimenti
- Area manifatturiera
- Servizi postali e corrieri
- Organizzazioni di ricerca

Profilo Aziendale



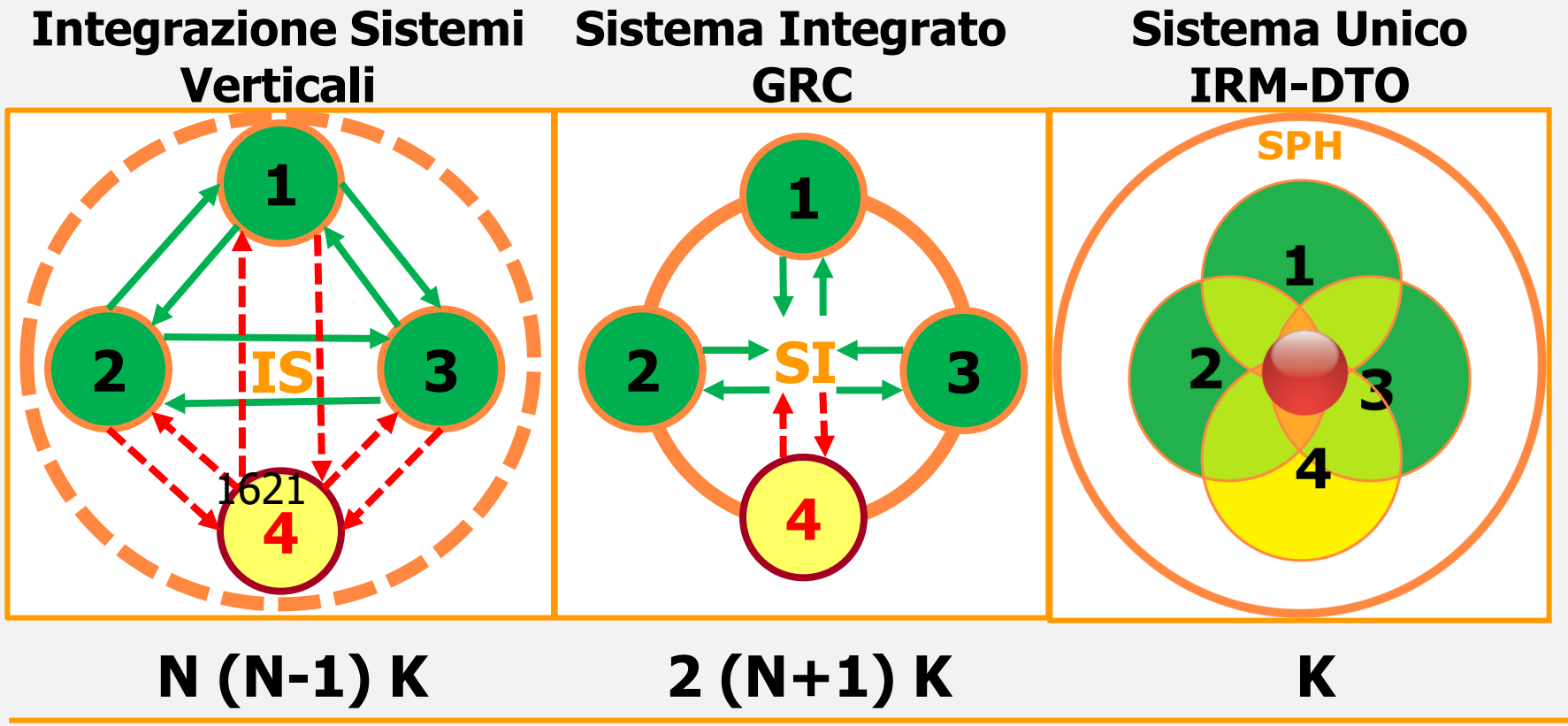
* Media del livello Customer Satisfaction dal 2007

ISO 9001 BUREAU VERITAS Certification

ISO 26000 SOCIAL RESPONSIBILITY

ISO 27001 BUREAU VERITAS Certification

Visione e Missione



Articolo AIIA «L'Evoluzione dei Sistemi Software per i Controlli Interni»

Market Guide: DTO – Case study su IRM/GRC

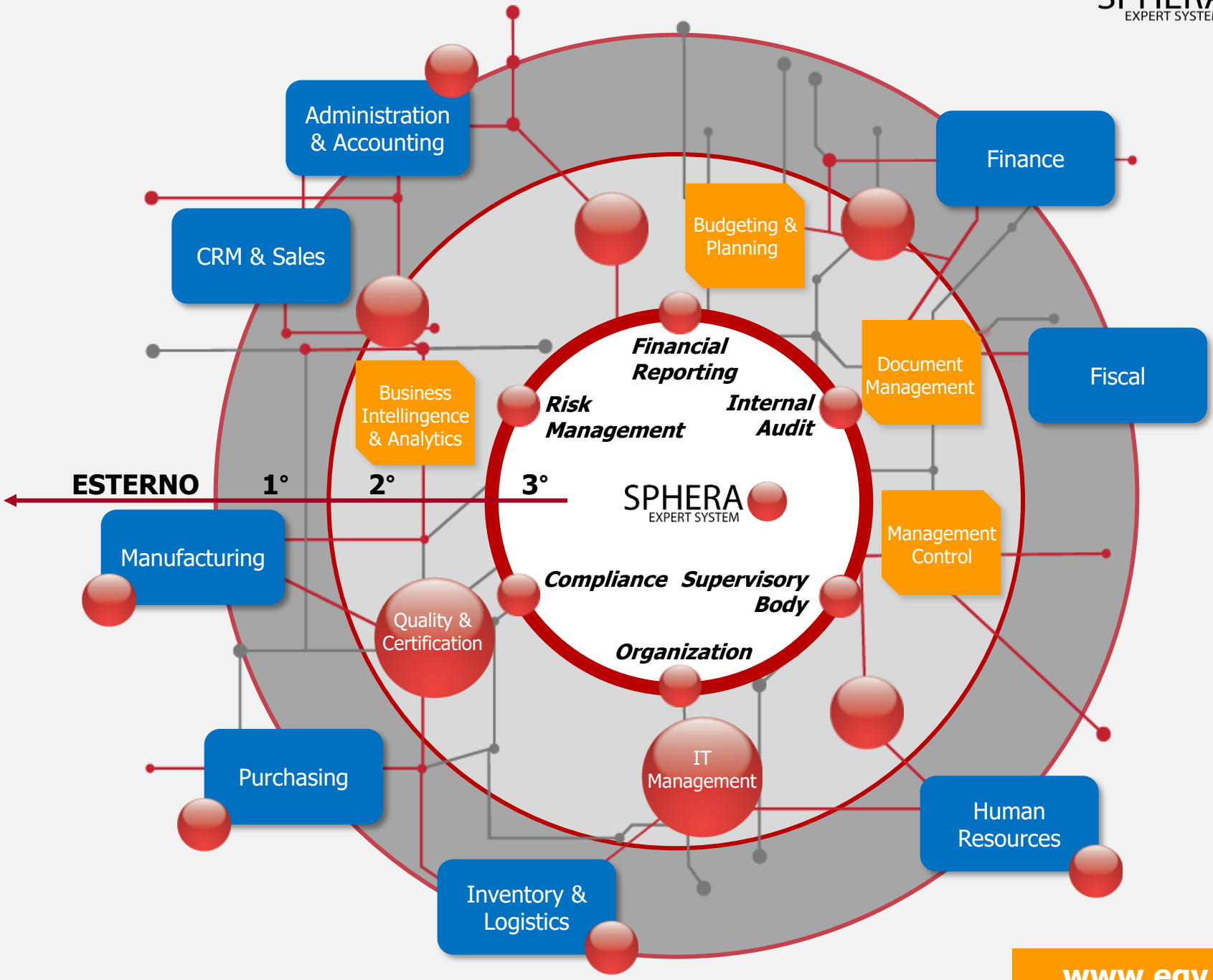
Architettura

3° LIVELLO (Governance)
Copre l'intera operatività di ogni funzione di Controllo e fornisce una gestione realmente integrata dello SCI.

2° LIVELLO (Management)
Fornisce strumenti e tecnologie per integrare, interfacciare o realizzare l'intero perimetro di controlli, certificazioni e attività di gestione e analisi.

1° LIVELLO (Operational)
Si interfaccia agevolmente con i sistemi del Business per consentire la pianificazione di controlli puntuali e a distanza.

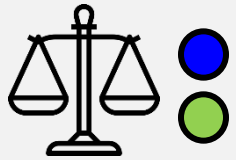
AMBIENTE ESTERNO
Fornisce strumenti per l'analisi a distanza e il controllo dei fenomeni.



Implementazioni

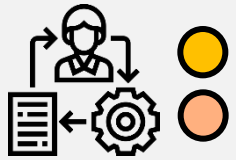
- Valutazione dello SCI
- Internal Audit
- Controlli Ispettivi
- Validazione Prudenziale (SREP)
- Quality Assurance (QAIP)
- Compliance (Legal Inventory)
- Dirigente Preposto (262)
- Modello Organizzativo (231)
- Certificazioni Aziendali (ISO)
- Salute e Sicurezza sul Lavoro (SSL)
- Whistleblowing
- Privacy (GDPR)
- Rating di Legalità
- Sistema di Gestione Ambientale (SGA)
- Risk Management
- Control Risk Self Assessment (CRSA)
- Rischi Operativi
- Perdite Operative (LDC - DIPO)
- Identificazione Frodi

- Criticità e piani d'azione
- Monitoraggio del Credito
- Controlli a Distanza
- Controlli di Linea (Fenomeni)
- Antiriciclaggio (MOAR)
- Gestione pareri
- Informazioni Privilegiate
- Operazioni Parti Correlate
- Controversie Clientela
- Cause Passive
- IT (CyberSecurutyFramework)
- IT Risk (COBIT, ITIL)
- Data Quality
- Documentale
- Gestione Progetti e Risorse
- Controllo di Gestione
- Qualifica Fornitori e Forniture
- Deleghe e Responsabilità
- Crisi d'Impresa



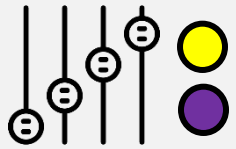
AMBITO LEGALE

Supporto interpretativo della normativa di riferimento



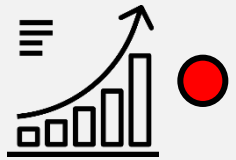
AMBITO ORGANIZZATIVO

Supporto all'organizzazione per la gestione dei cespiti e dei processi



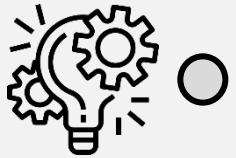
AMBITO DI CONTROLLO

Supporto nei sistemi di controllo interni e nelle valutazioni organizzative e dei processi



AMBITO BUSINESS

Supporto nell'attività di verifica dei dati operativi, economici e finanziari dell'azienda



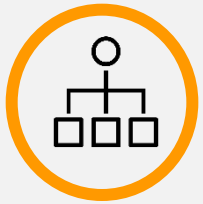
AMBITO TECNOLOGICO

Supporto nell'attività di integrazione e implementazione soluzioni

Funzionalità Tecniche*


Multi-
Organizzazione


Multi-
Lingua


Multi-
Funzionale


Completamente
Web

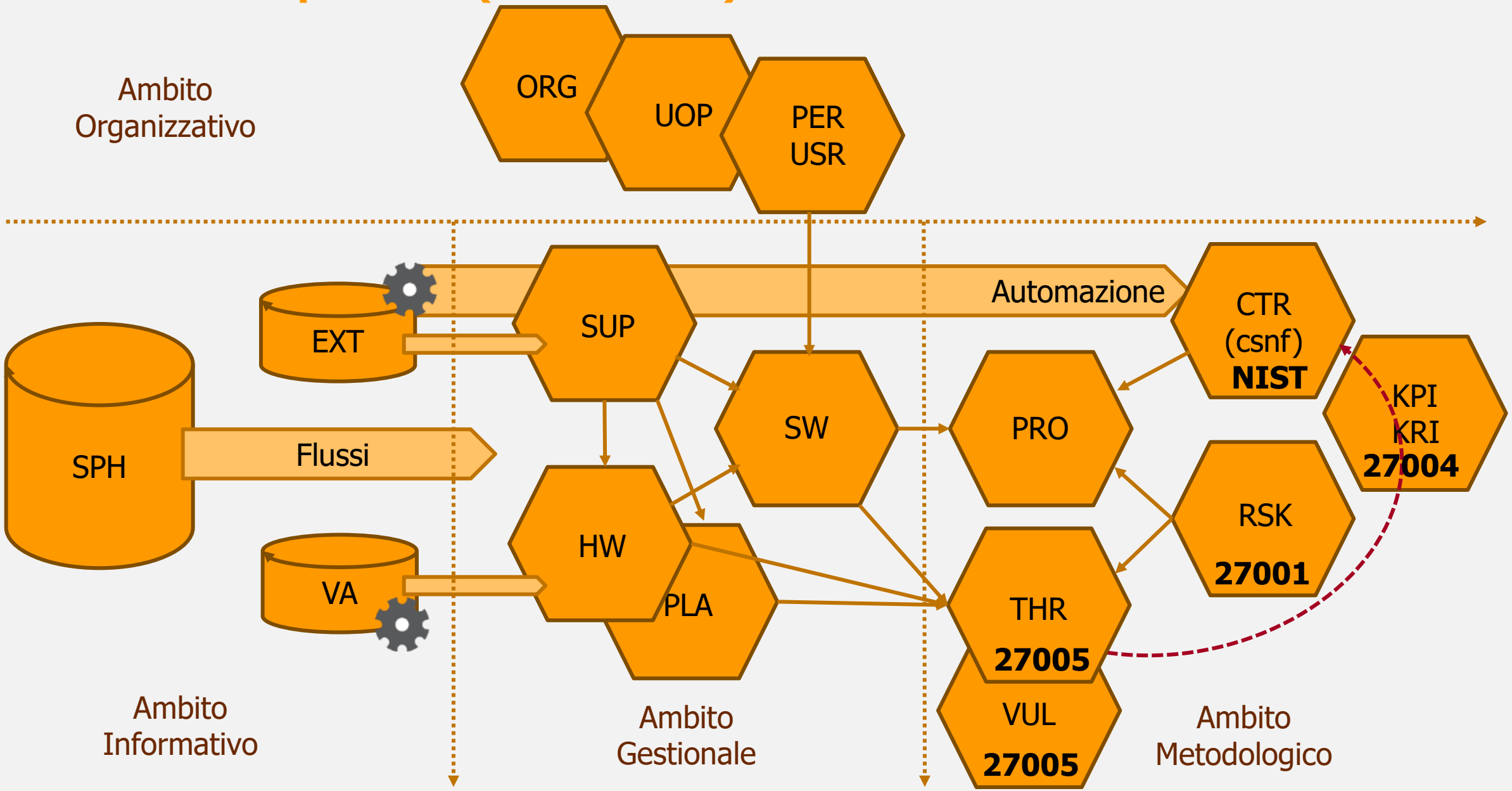

Single
Sign-On


Integrazione
Web Service

1. Gestione cataloghi e relazioni (Assessment)
2. Strutturazione contenuti informativi
3. Integrazione a flussi esterni (ETL)
4. Riorganizzazione dati (DWH)
5. Gestione avanzata profili utenti
6. Definizione modelli di gestione e controllo
7. Strutturazione flusso attività (WFL – BPMN 2.0)
8. Configurazione schemi di rilevazione
9. Pianificazione attività
10. Programmazione attività e risorse
11. Gestione attività di rilevazione
12. Monitoraggio flusso attività
13. Gestione cruscotti di analisi (BI)
14. Lavorazione flussi (CAD)
15. Produzione run-time report
16. Documentale (DAA)
17. Segnalazione scadenze allarmi (HP)
18. Comunicazione extra sistema (Mail)
19. Chat proattiva
20. Rendicontazione attività (Time keeping)
21. Schedulazione attività, condivisione e agenda
22. Ticket
23. News e Help contestuale (Chatbot)
24. AI (previsioning and pattern recognition)

*__SPHERA_Presentazione__ per ulteriori dettagli

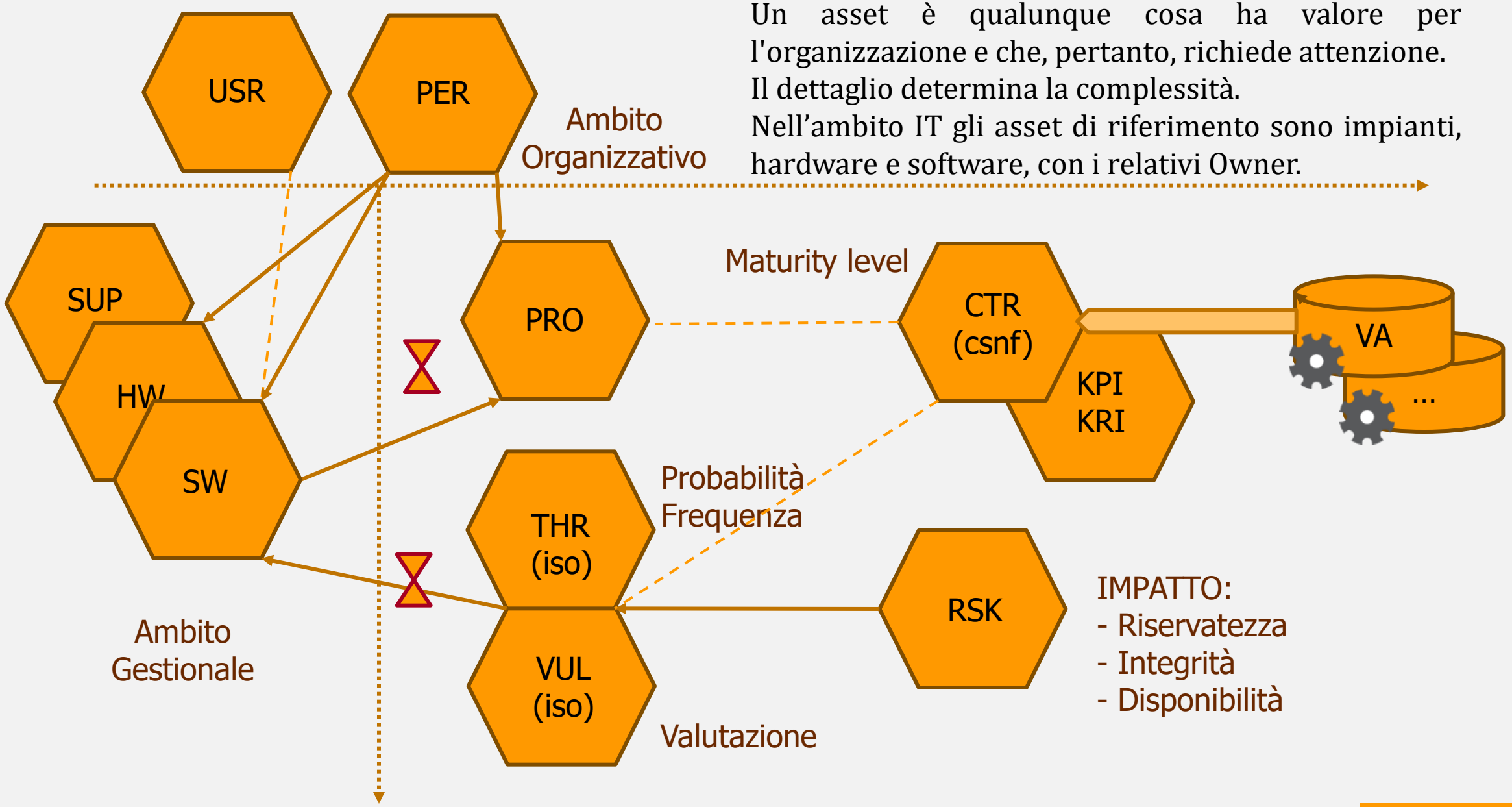
Il modello complessivo (Controlli IT)



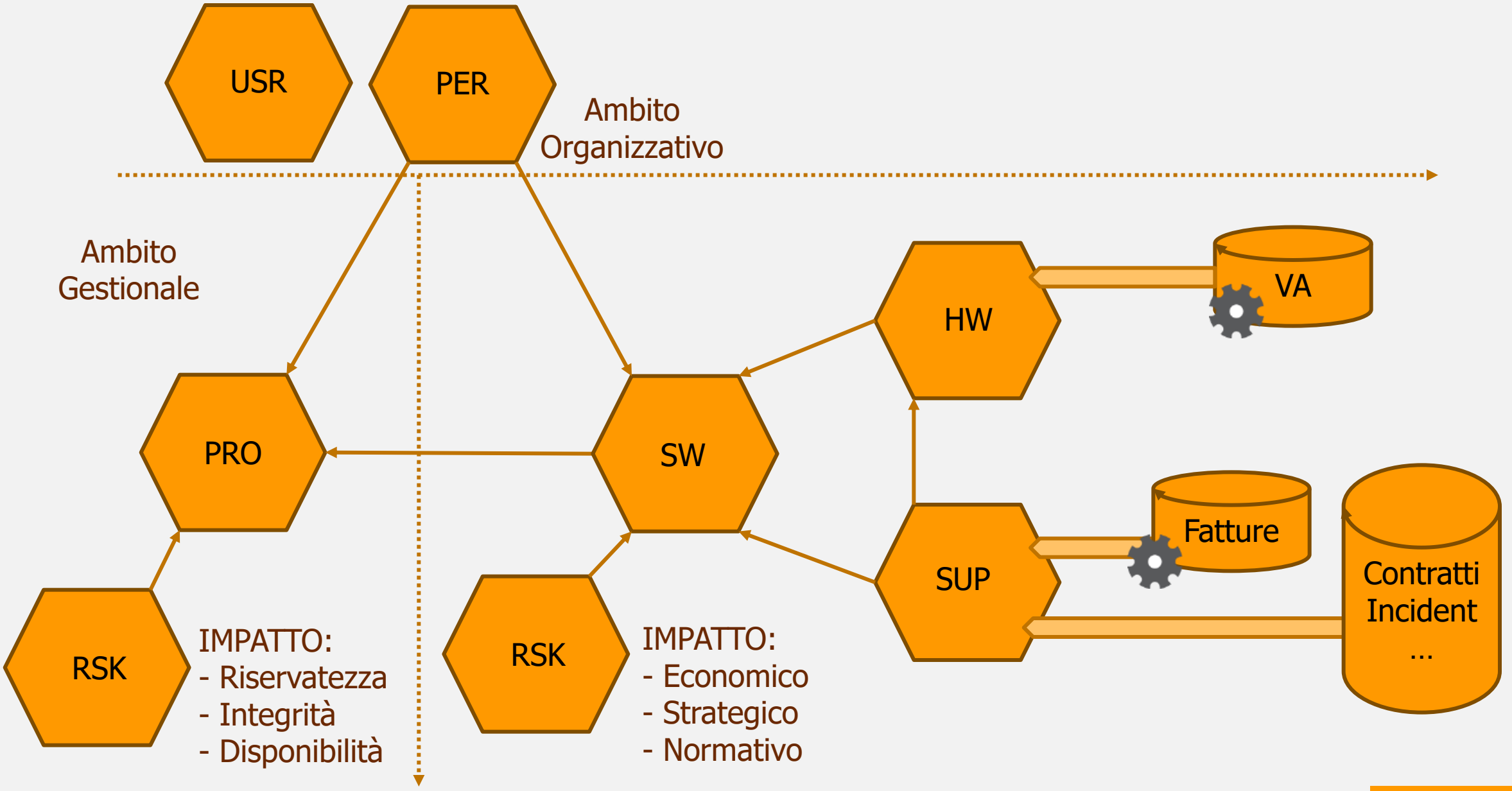
Risk Assessment (Rischio IT)

ISO 27005 - 8.2.2 Identification of assets

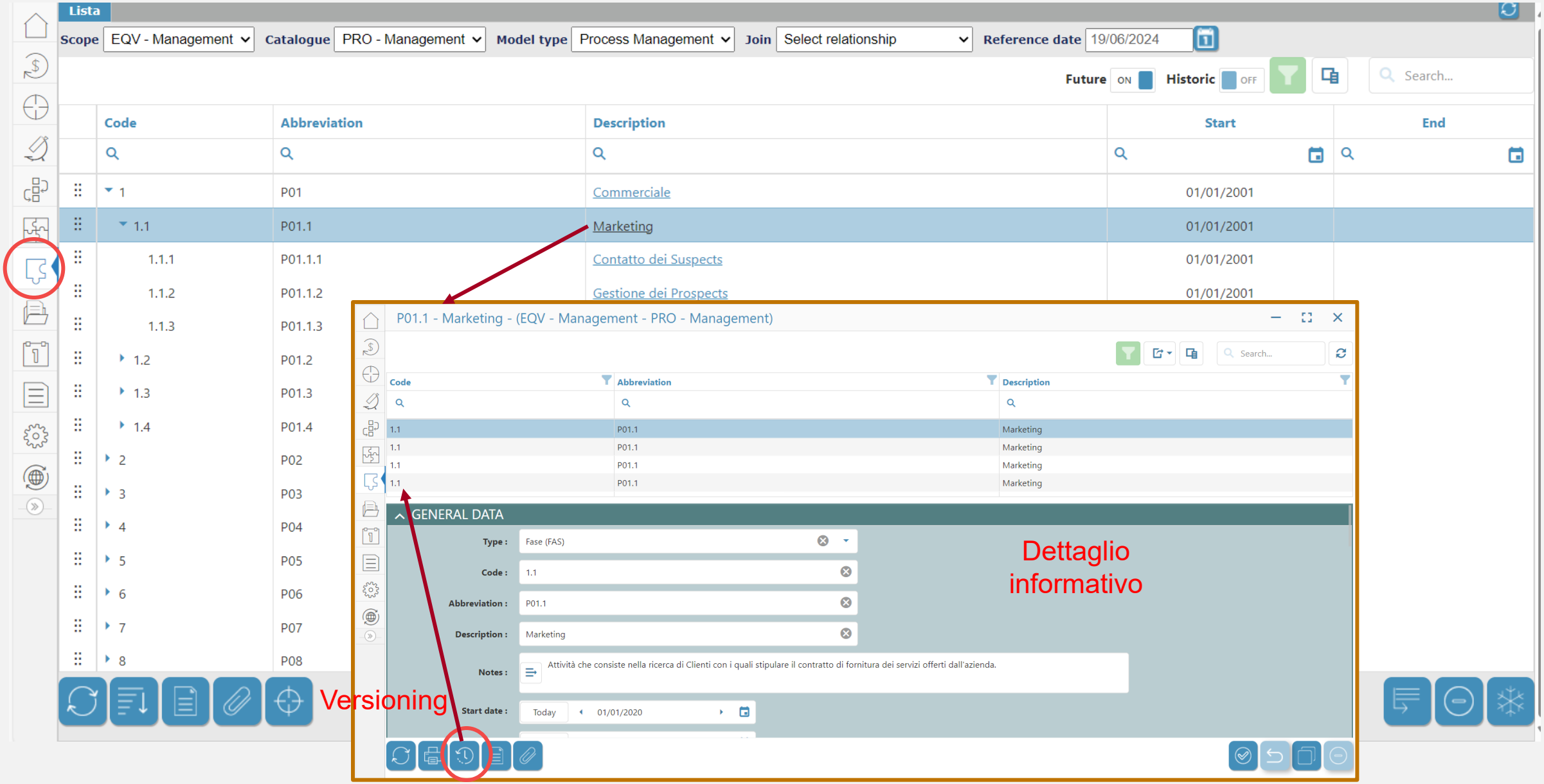
Un asset è qualunque cosa ha valore per l'organizzazione e che, pertanto, richiede attenzione.
Il dettaglio determina la complessità.
Nell'ambito IT gli asset di riferimento sono impianti, hardware e software, con i relativi Owner.



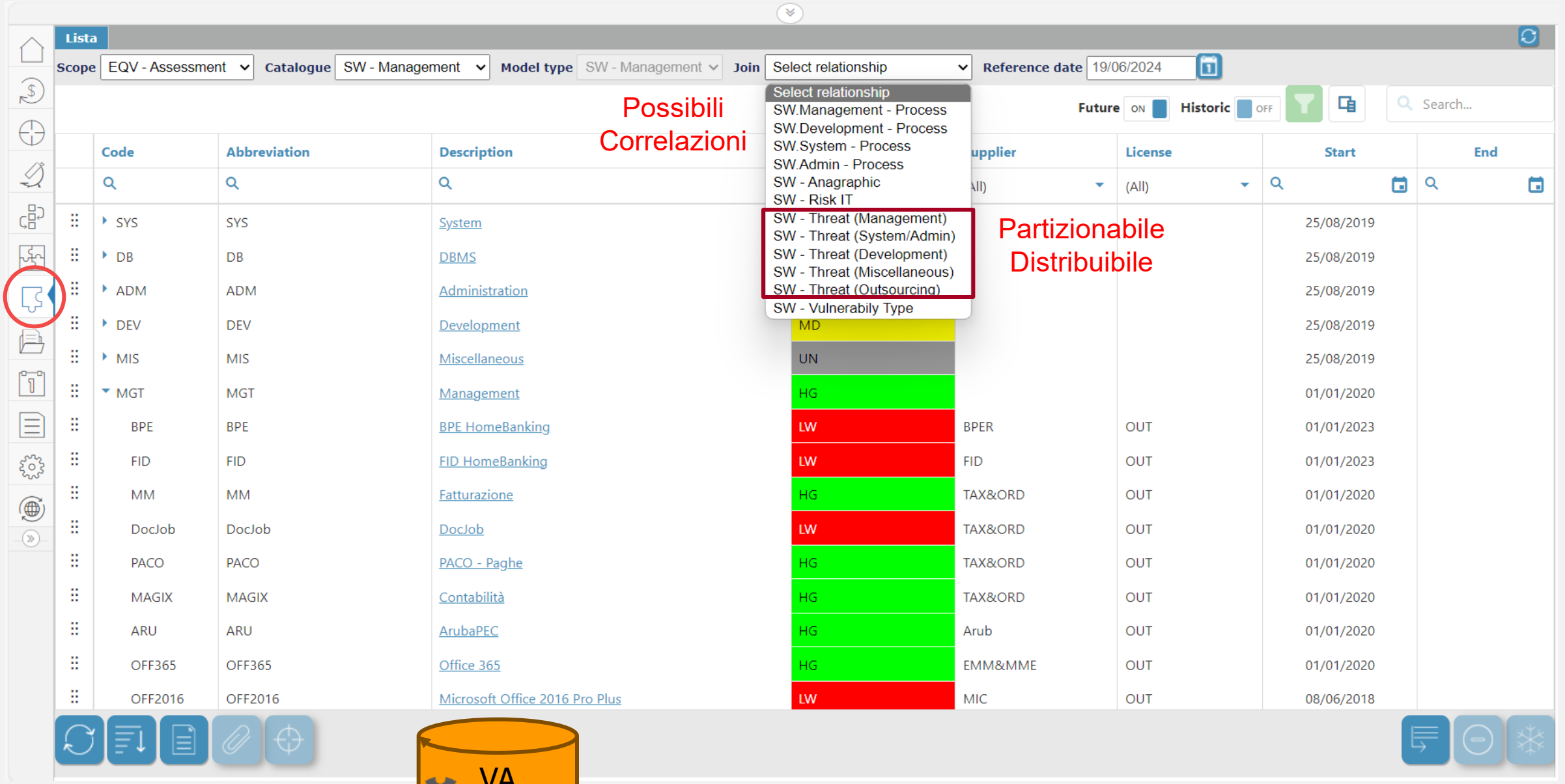
Business Impact Analysis



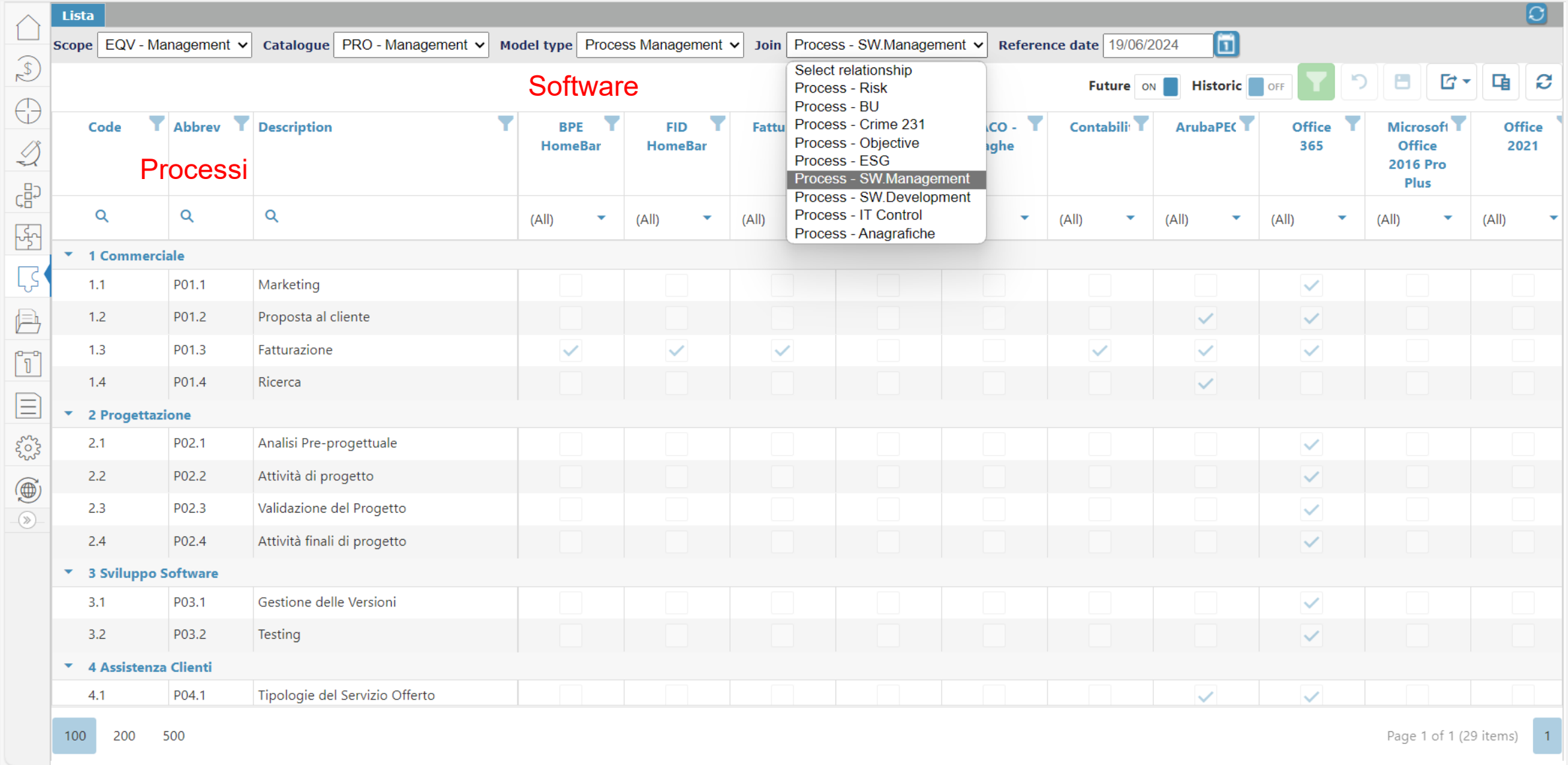
Catalogo Processi



Catalogo Software



Relazione Processi - Software



Catalogo Hardware

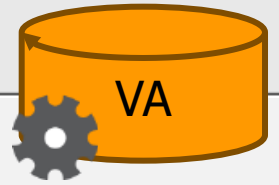
SPHERA EXPERT SYSTEM

Control type EQV - Development **Model** HW - Management **Model type** HW - Management **Join** Visualizzazione catalogo

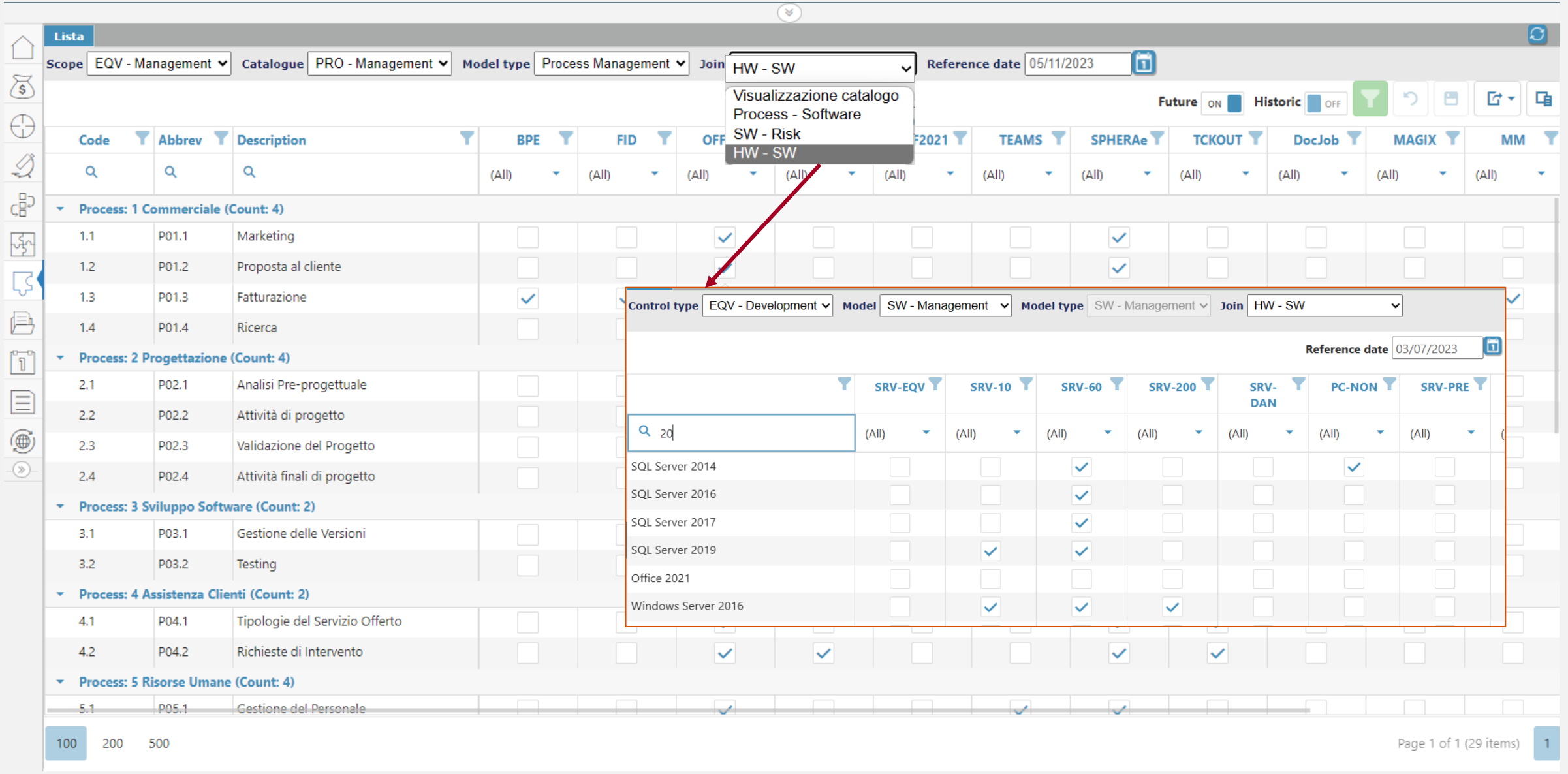
Reference date 03/07/2023 **Future** ON **Historic** OFF Search...

Code	Abbreviation	Description	Assignement	Location	Owner	Start	End
			(All)	(All)	(All)		
SRV	SRV	Server				11/06/2018	
SRV-EQV	SRV-EQV	SRV EQV (main)	TUB	SRV	EQV	11/05/2020	
SRVEQV10	SRV-10	SRVEQV 10 (Client)	TUB	SRV	EQV	14/06/2019	
SRVEQV60	SRV-60	SRVEQV 60 (DB)	TUB	SRV	EQV	14/06/2019	
SRVEQV200	SRV-200	SRVEQV 200 (Test)	TUB	SRV	EQV	14/06/2019	
SRV-DAN	SRV-DAN	Server VPN (DAN)	DAN	PRJ.R1	EQV	18/09/2019	
SRV-PRE	SRV-PRE	SERVER-Presenze	TUB	HAL	EQV	31/05/2023	
PC	PC	Personal Computer				11/06/2018	
PC-HP-NON	PC-NON	HP NON ASSEGNATO	DAN	PRJ.R1		12/06/2019	
PC-EQV-TAU	PC-TAU	PC-EQV-TAU	TAU	DEV.R2		12/06/2019	
PC-SAM-NON	PC-NON	NON ASSEGNATO-SAMSUNG		HOM		20/11/2019	
PC-EQV-ERC	PC-ERC	PC-EQV-ERC	ERC	HOM		22/07/2021	
PC-EQV-FIL	PC-EQV-FIL	PC-EQV-FIL		HOM		22/07/2021	
PC-EQV-DEM	PC-DEM	PC-EQV-DEM	DEM	HOM		18/10/2021	

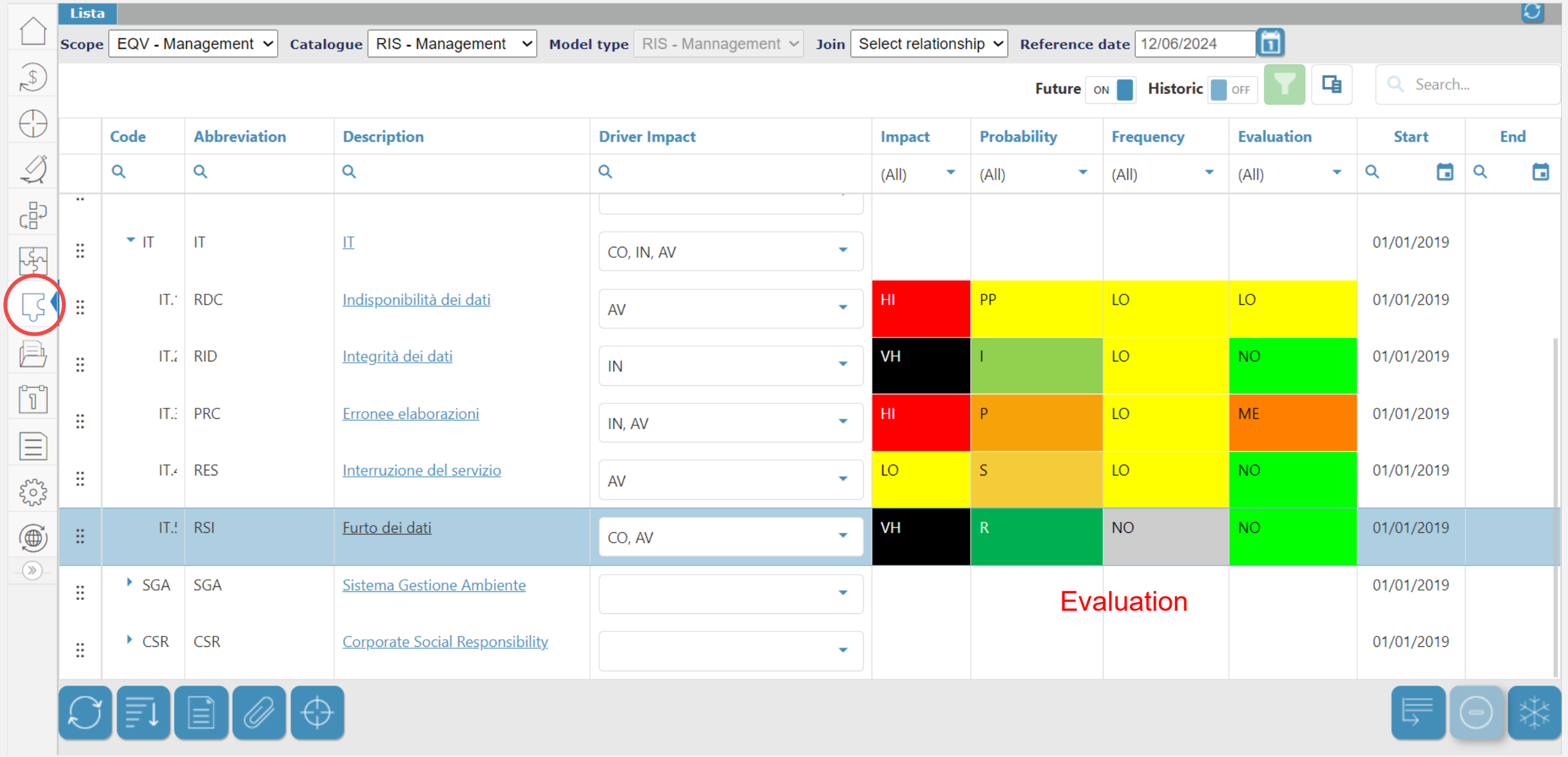
Assessment HW - Risk



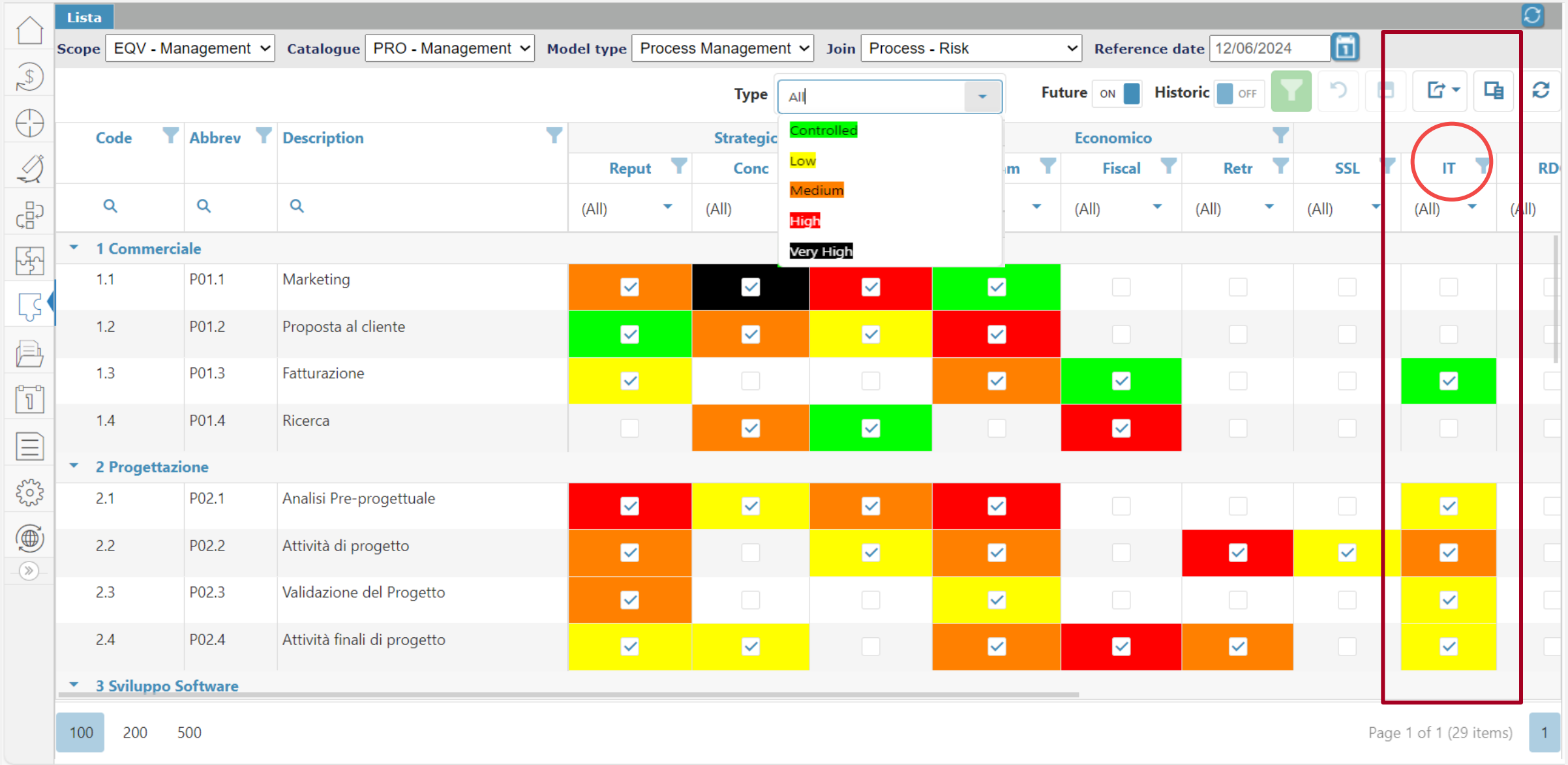
Relazione Hardware - Software



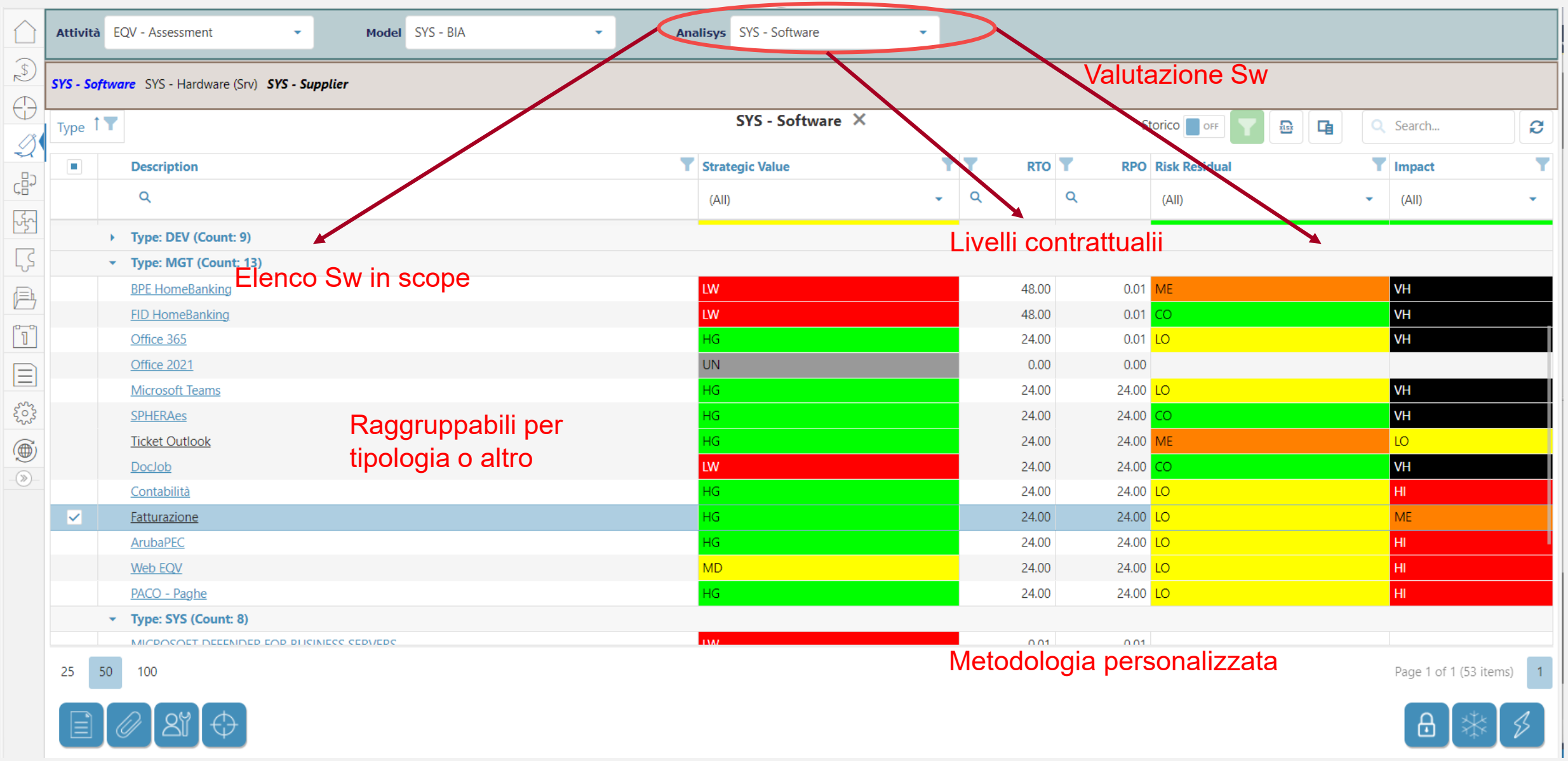
Catalogo Rischi (IT Focus)



Relazione Processi – Rischi (IT Focus)



IT - BIA – Software Assessment



IT - BIA – Software Assessment

SPHERA EXPERT SYSTEM

SYS - Software --> Fatturazione

GENERAL DATA

RELATIONSHIP

Valutazione Processi

Process :

Code	Description	Potential risk	Control evaluation	Residual Risk	Evaluation KPI
		(All)	(All)	(All)	(All)
1.3	Fatturazione	ME	AD	LO	S
7.2	Acquisti	ME	IM	ME	

Valutazione Trattamenti (DPO)

DPO Registry :

Sotto-Finalità	Data Category	Priority
		(All)
Personalizzazione proposta e comunicazione esterna	Comune	ME
Elaborazione fatture e gestione pagamenti	Comune	HI
Pianificazione, gestione e comunicazione del progetto	Comune	HI

HardWare

Hardware :

Codice	Descrizione	Supplier	RTO	RPO
		(All)		
PC-EQV-BEL	PC-EQV-BEL	EQV	24.00	24.00

CONTRACT

RTO : 24.00

RPO : 24.00

License : Outsourcing (OUT)

Expiry : Today

Numero : 0

Cost : 0.00

Vulnerability :

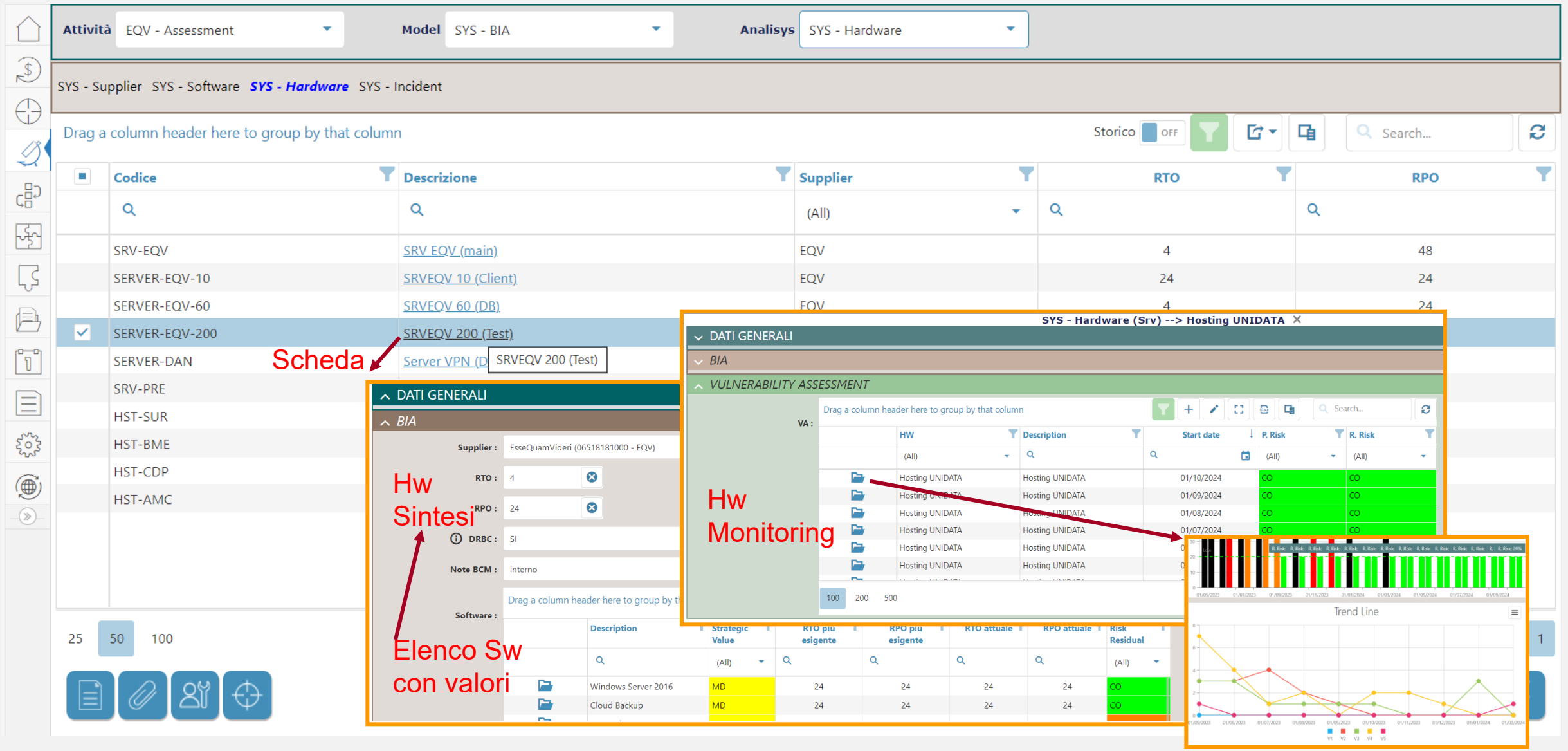
Description	Strategic Value	Likelihood of occurence - Threat	Easy to Exploitation	Evaluation
	(All)	(All)	(All)	(All)
Well-known flaws in the software	HG	HI	HI	VH
Complicated user interface	HG	ME	LO	ME
Immature or new software	HG	ME	ME	ME

Resource :

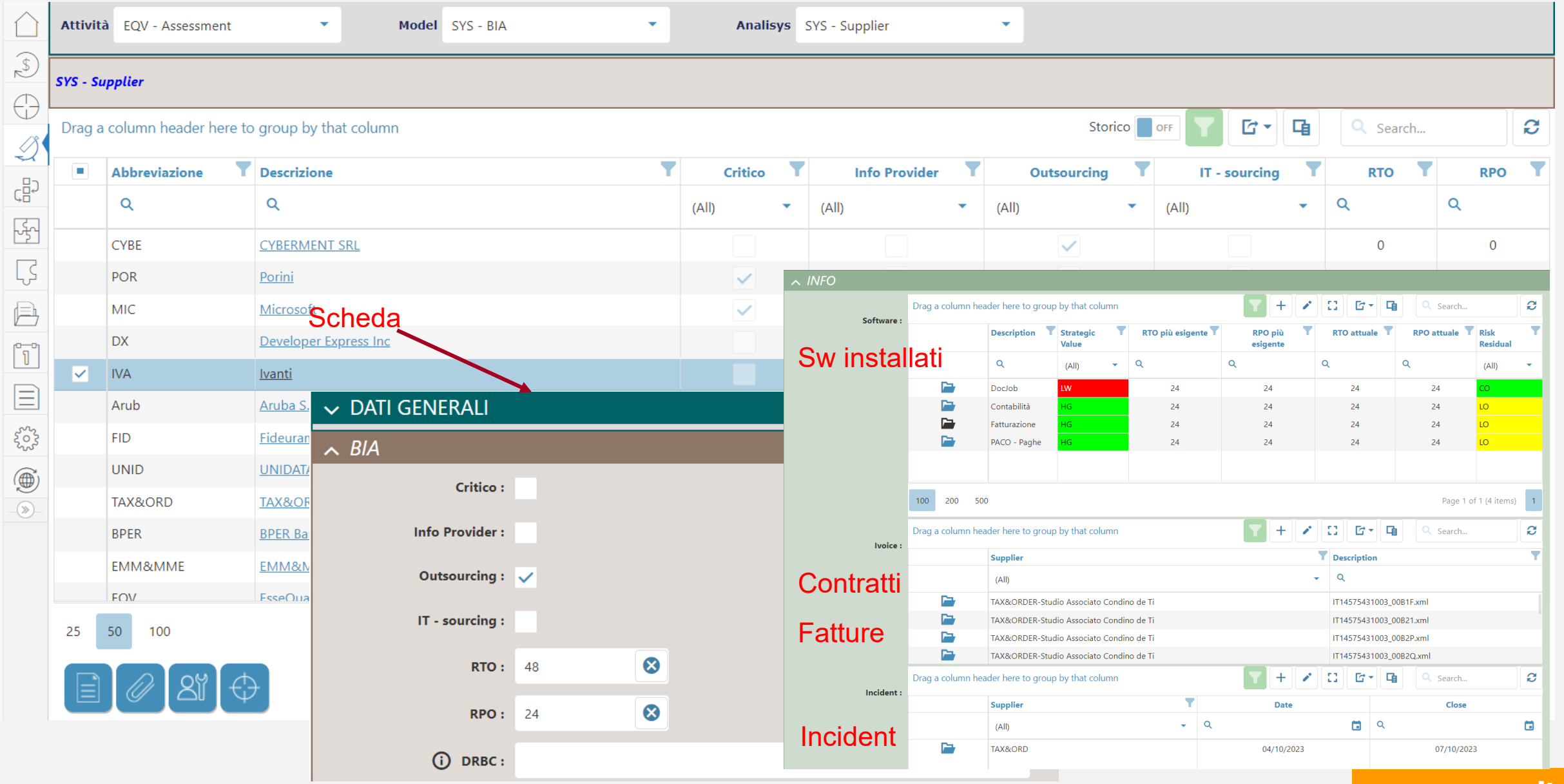
Resource	In Giornata	A GG + 5	A GG + 10	Entro il mese
	(All)	(All)	(All)	(All)
Belloni Rino	NO	NO	NO	HI
Taticchi Walter	NO	NO	LO	ME
Cardarelli Giorgio	NO	NO	LO	ME
D'Anzilio Francesco	NO	LO	ME	HI
Casturani Enrico	NO	LO	ME	HI
Tubaro Stefano	NO	LO	ME	HI

100 200 500 Page 1 of 1 (8 items) 1

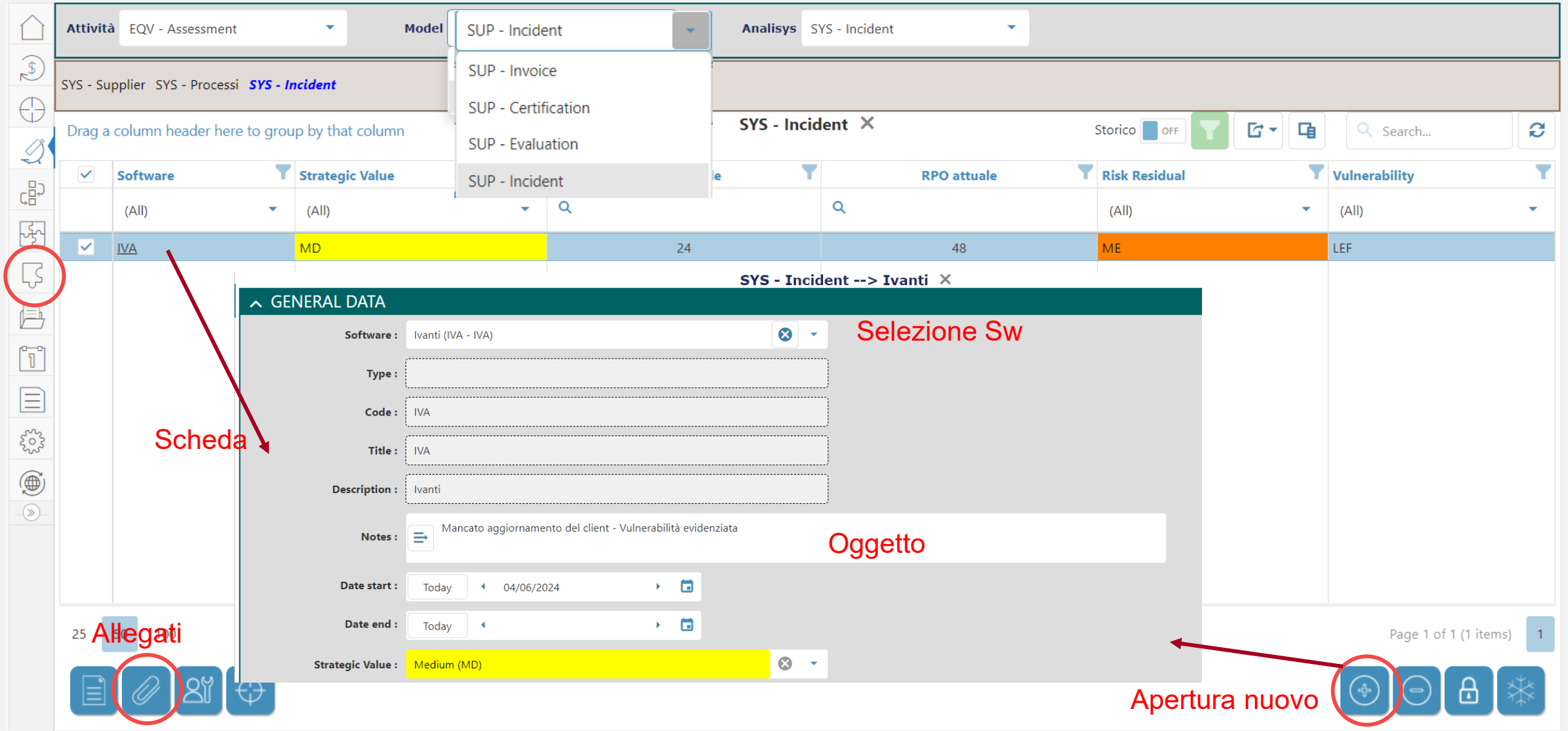
IT - BIA – Hardware Assessment



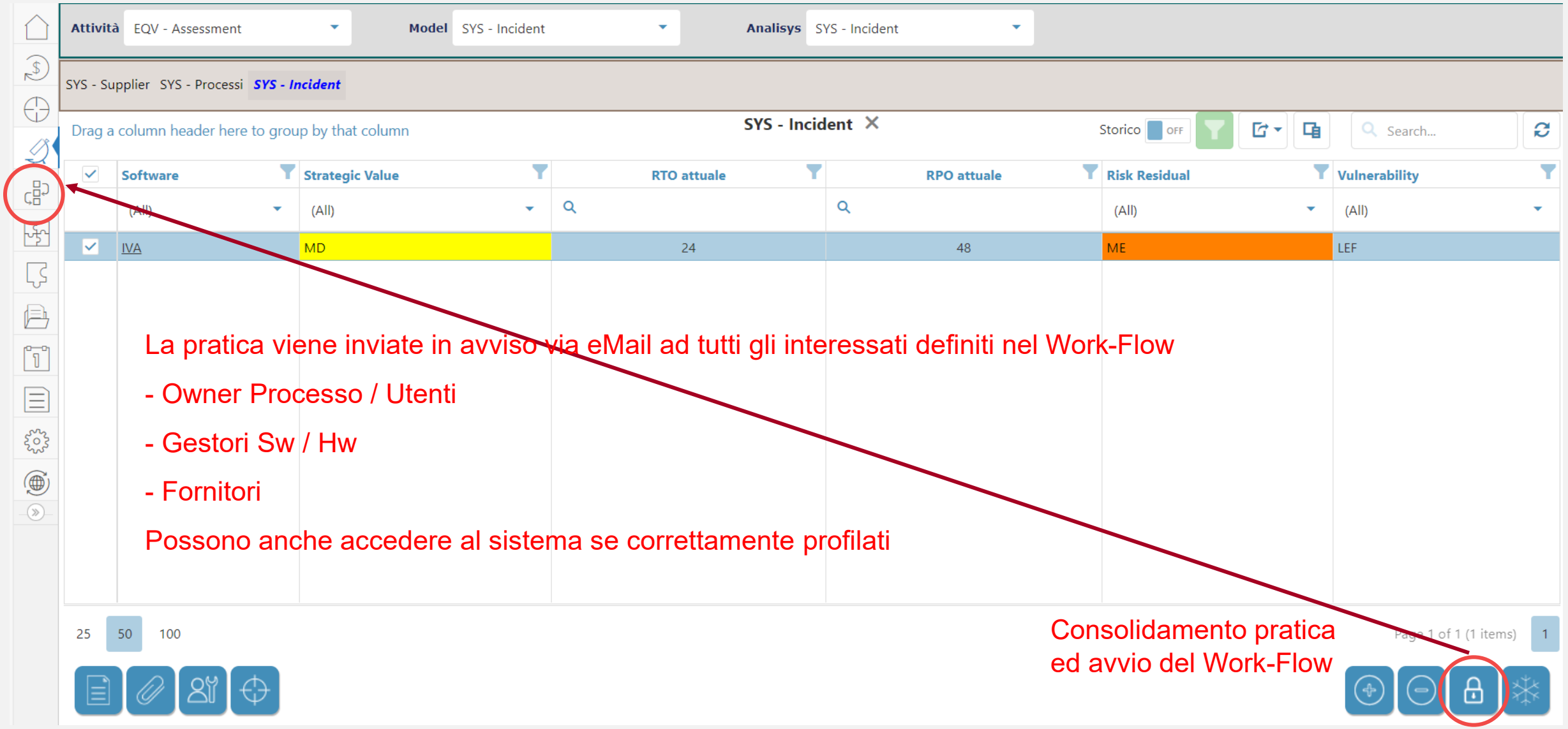
IT - BIA – Supplier Assessment



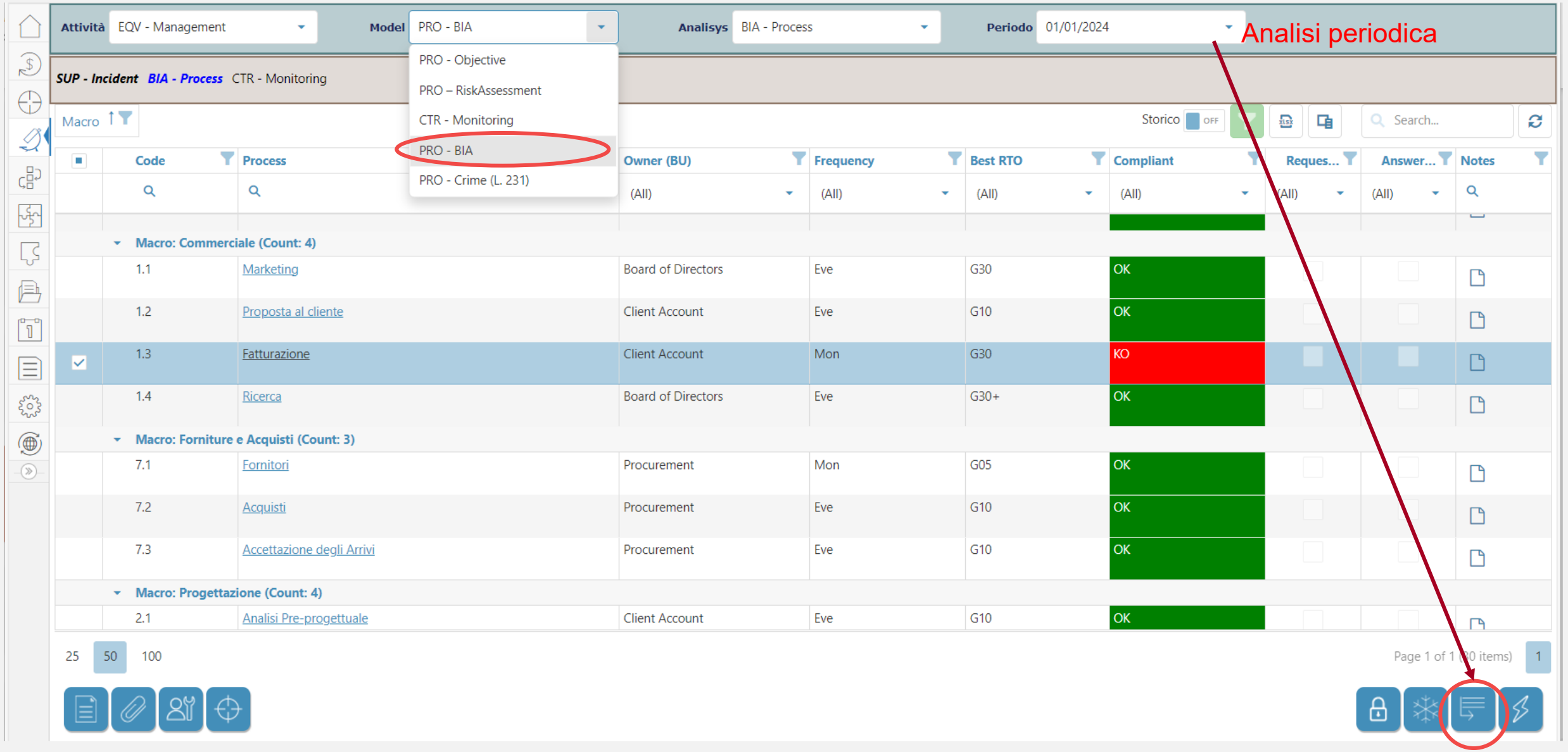
Supplier – Incident (apertura)



Supplier – Incident (Work-Flow)



Management – BIA - Processi



Management – BIA - Processi

SPHERA EXPERT SYSTEM

GENERAL DATA

CARATTERISTICS

IMPACT

Best RTO : 1 Mese (entro 1 Mese) (G30)

Evaluation :

Drag a column header here to group by that column

	Evento	Strategic	Economic	Compliance
	(All)	(All)	(All)	(All)
	G (entro fine giornata)	None	None	None
	G+5 (entro il 5° giorno)	None	None	None
	G+10 (entro il 10° giorno)	None	None	None
	1 Mese (entro 1 Mese)	None	Low	None
	> 1 Mese	None	Medium	None

100 200 500

Compliant : Not Compliant (KO)

SUPPORT

INVOLVED RESOURCES

SUPPORT

Software :

	Acro...	Description	R...	RTO need	RPO	RPO need	Compliant
	BPE	BPE HomeBanking	48.00	48.00	24.00	24.00	OK
	FID	FID HomeBanking	24.00	24.00	24.00	24.00	OK
	MM	Fatturazione	24.00	24.00	24.00	24.00	OK
	MAGIX	Contabilità	24.00	24.00	24.00	24.00	OK
	ARU	ArubaPEC	24.00	24.00	24.00	0.01	KO
	SPH.EQV	SPHERAes EQV	24.00	24.00	24.00	24.00	OK

Hardware :

	Abbreviazione	Descrizione	RTO	RTO need	RPO	RPO need	Compliant
	SERVER-EQV-10	SRVEQV 10 (Client)	4.00	48.00	24.00	24.00	OK
	PC-BEL	PC-EQV-BEL	24.00	24.00	24.00	24.00	OK

Outsoucer :

	Sigla	Descrizione	Critic	RTO	RTO need	R...	RPO need	Compliant
	EQV	EsseQuamVideri		2.00	2.00	24.00	24.00	OK
	Arub	Aruba S.p.A.	✓	24.00	24.00	24.00	24.00	OK
	FID	Fiduciaria Investimenti Società		24.00	24.00	0.00	0.00	OK
	TAX&ORD	TAX&ORDER-Studio Associato	✓	48.00	48.00	24.00	24.00	OK

Risultanze

RACI

Codice	Abbreviazione	Business Unit	RACI
		(All)	(All)
	BoardDir	Board of Directors	Informed
	AdmAcc	Administrative-Accounting	Accountable
	CliAcc	Client Account	Responsible

	Resource	In Giornata	A GG + 5	A GG + 10	Entro il mese
		(All)	(All)	(All)	(All)
	Belloni Rino	No	No	Si Titolare	Si Titolare
	Taticchi Walter	No	No	Si BackUp	Si BackUp
	Cardarelli Giorgio	No	No	Si BackUp	Si BackUp

Perché SPHERAes (estratto ultima rivista AIIA)

SPHERA EXPERT SYSTEM

Diffondere tecnologia per innovare il sistema integrato dei controlli interni

PERCHE' SCEGLIERE SPHERA EXPERT SYSTEM

- Produttori e Utilizzatori del Software
- Progettazione ed Assistenza Diretta
- 100% Progetti con Successo
- 30 Anni di Esperienza
- Rapporto a Lungo Termine con i Clienti



- Tecnologia DTO e GRC
- Scalabilità, Flessibilità e Adattamento
- Aggiornamento Tecnologico Continuo
- Integrazione con Qualsiasi Sistema
- Riduzione Total Cost Ownership IT

Grazie

Ulteriori informazioni:

www.eqv.it

Contatti:

Rino Belloni – CEO

rino.belloni@eqv.it

Ercole Belloni – Innovation Manager

ercole.belloni@eqv.it