

## Reports, Tables and Graphics to support specific activities

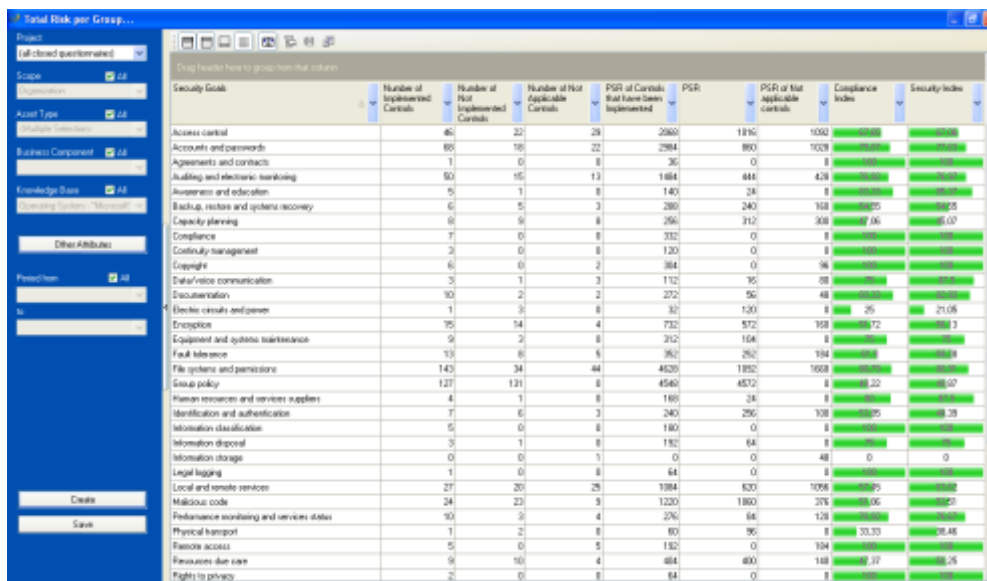
Part of the Risk Management process, reports, tables and graphics generation are fundamental to support the decision making, provide for action plans and facilitate awareness process by Senior Management and operating teams.

Modulo Risk Manager generates graphics, as well as technical and executive reports supporting different activities for the organization security control and management. Let's see some of these activities:

### Identifying areas with highest risk level

One of the most difficult tasks is to identify top risk areas and prioritize mitigation and control actions. Using the “**Total Risk per Group**” table, is possible to identify, in a consolidated way, top risk areas that are the main focus of organizations.

The example below shows a Total Risk per Group table.



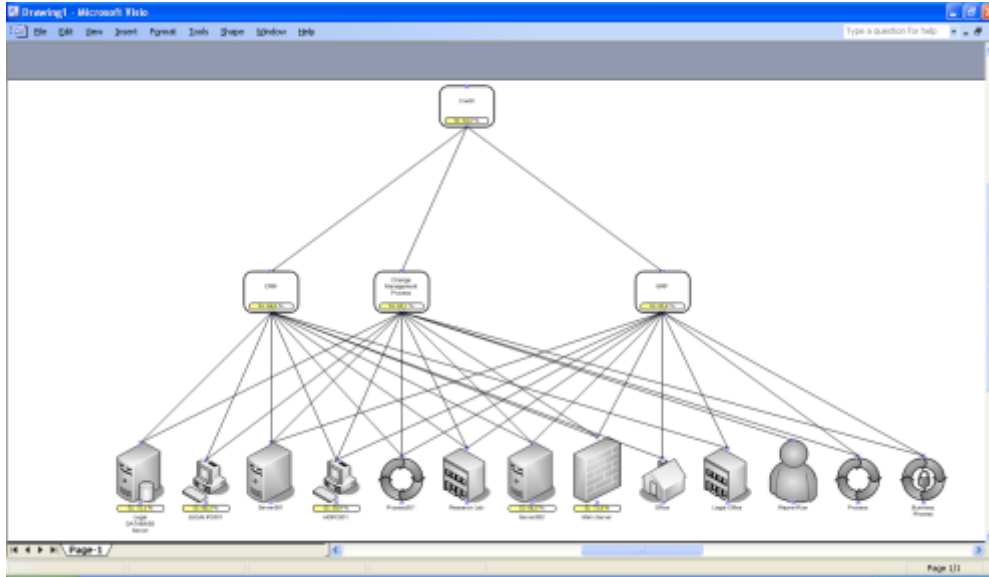
Security Goals	Number of Implemented Controls	Number of Not Implemented Controls	Number of Not Applicable Controls	PSR of Controls that have been implemented	PSR	PSR of Not applicable controls	Compliance Index	Security Index
Access control	46	22	29	2660	1816	1000	100%	100%
Access and controls	86	18	22	2984	860	1000	100%	100%
Agreements and contracts	1	0	0	36	0	0	0%	0%
Building and electronic monitoring	82	16	13	1484	444	429	100%	100%
Awareness and education	5	1	0	140	24	0	100%	100%
Backup, restore and systems recovery	6	5	3	280	240	168	100%	100%
Capacity planning	9	9	8	296	312	308	100%	100%
Compliance	7	0	0	332	0	0	100%	100%
Continuity management	2	0	0	120	0	0	100%	100%
Copyright	6	0	2	384	0	96	100%	100%
Data/voice communication	3	1	3	132	36	0	100%	100%
Dissemination	10	2	2	272	56	48	100%	100%
Electric cables and cables	1	3	0	36	180	0	25%	21.6%
Encryption	95	14	4	376	572	168	100%	100%
Equipment and systems maintenance	9	2	0	212	154	0	100%	100%
Facilities	13	0	0	362	262	194	100%	100%
File systems and permissions	143	34	44	4620	1892	1668	100%	100%
Group policy	127	131	0	4540	4572	0	100%	100%
Human resources and services suppliers	4	1	0	168	24	0	100%	100%
Identification and authentication	7	6	3	240	296	108	100%	100%
Information classification	5	0	0	180	0	0	100%	100%
Information disposal	3	1	0	132	64	0	100%	100%
Information storage	0	0	1	0	0	48	0%	0%
Legal logging	1	0	0	64	0	0	100%	100%
Local and remote services	27	20	29	1084	620	1006	100%	100%
Malicious code	24	23	3	1200	1880	376	100%	100%
Performance monitoring and services status	10	3	4	296	84	128	100%	100%
Physical transport	1	2	0	60	96	0	100%	100%
Remote access	5	0	0	182	0	194	100%	100%
Resources due care	9	10	4	364	480	148	100%	100%
Rights to privacy	2	0	0	64	0	0	100%	100%

Based on this table, your organization also can prioritize action and investments to mitigate risks.

### Identifying Risks per Business Component

Using report “**Business Components Integration View**” is possible to gather strategic information in a graphic format to help identify risks. In example below, a report focused on the “**Credit**” Business Process was produced. In a single report, you gather information such as:

- Security Index, Risk Index, Compliance Index or Non-Compliance Index for the focused Business Process;
- Inventory of System and Services supporting the business and its Security Index;
- Inventory of Assets with their Security Index



## Identify Risks status in each Control

With table **“Risk Status in Control”** Modulo Risk Manager provides information of controls and helps generate action plans to implement controls and mitigate risks. It is also possible to gather evidences for implemented controls. These evidences include configurations and parameters developed during the Automatic Evidence Collection (Automatic Collectors) or responses to Web Interviews. This resource also helps both internal and external audit processes.

Group	Control	Asset Type	Evidence	Comments
Accounts and passwords	In Windows XP Professional, highly-privileged accounts should only be used for administrative operations.	Technology	Administration Group Info . Description: Administrators have complete and unrestricted access to the computer/Domain . Caption: MSS-FU008\Administrators . Accounts: Element 1: Caption: MSS-FU008\admservp Description: Bulk-in account for administering file computer/Domain FullName: ... Element 2: Caption: MSS\Facators Description: Estigalro - Security Lab FullName: Thiago Soares . Subgroups: Element 1: Caption: MSS\Domain Admins Description: Designated administrators of the domain	
Updates/patches	Windows XP Professional patches released by Microsoft should be installed.	Technology	Patches™ status (MPSA scan results)	
Group policy	The "Maximum Password Age" parameter should be assigned a value ranging from 30 to 98 days.	Technology	Local Security Policy -> Security Settings -> Account Policies -> Password Policy Maximum password age : 98 days [ OK ]	
Group policy	The "Maximum Password Length" parameter should be set to 14.	Technology	Local Security Policy -> Security Settings -> Account Policies -> Password Policy Minimum password length : 14 characters [ OK ]	
Encryption	Sensitive information stored in a harddisk in Windows XP Professional should be protected by encryption.	Technology	Local Security Policy -> Local Policies -> Security Options Send unencrypted passwords to third-party SMB servers : Disabled	
Group policy	The "Microsoft network server: Amount of idle time required before suspending session" parameter should be set to the value 15.	Technology	Local Security Policy -> Local Policies -> Security Options Amount of idle time required before suspending session : 15 minutes [ OK ]	