## **Selecting Domain-Specific Controls**

Policy authors identify risks in different domains that significantly impact their organization. Creating a control using the content wizard provides the freedom to select appropriate industry standards, frameworks, and regulatory controls. A user can choose a regulation to build controls that can be enforced implicitly within a domain. Stakeholders use the content pack to assess the standard controls and subcontrols by performing various workflow stage actions such as draft, test, and approve prior to control deployment.

## To select domain-specific controls:

- 1. Open RiskVision Enterprise Risk Manager.
- 2. Go to Risks > Controls and Questionnaires, and select the desired controls group.
- 3. Click Actions > New Controls with Content Wizard.

Create New Controls by Co	ntent Wizard	×
1. Regulations	Step 1: Select Regulations	* = required
2. Frameworks	Start with the Regulations that impact your organization. (Choices marked by * are not curr	ently
3. Domains	installed at your site. Please contact Agiliance Sales to purchase additional content.)	
4. Filters	Select one or more regulations Select All Clear All AB 1950 BASEL II California Privacy Law - CA 1386 FISMA GLB Act (15 USC Sec. 6801-6809) 16 CFR 314 HIPAA Sarbanes Oxley Credit Card Regulations - PCI Privacy Standards and Regulations Other Standards and Frameworks	
Cancel	< Bac	k Next >

The Regulations page in the Create New Controls by Content wizard.

4. Select one or more regulations, then click Next.

Create New Controls by Co	ntent Wizard	×					
1. Regulations	Step 2: Select Frameworks	* = required					
2. Frameworks	For each selected regulation, choose one or more frameworks you want to use for the co						
3. Domains	(Framework choices marked by * are not currently installed at your site. Please contact Agilia to purchase additional framework content.)						
4. Filters	FISMA       Select All       Clear All         □       FISMA*         □       NIST SP 800-53 (2007)*         ☑       NIST SP 800-53 (2009)         HIPAA       Select All         □       NIST 800-66*         □       NIST 800-66 (2008) with HITECH Act*         □       HIPAA (Part 164 - Security and Privacy)*         □       Agiliance 17799*         ☑       Agiliance 17799 HIGH_LEVEL						
Cancel	< Bac	ck Next >					

5.

The Frameworks page.

- 6. Click the checkbox next to all frameworks related to the regulations selected in the previous step.
- 7. Click Next.

Create New Controls by Co	ntent Wizard	X
1. Regulations	Step 3: Select Domains	* = required
2. Frameworks	Select Domains to assess for each selected Regulation and Framework.	
3. Domains	FISMA: NIST SP 800-53 (2009) Select All Clear All	~
4. Filters	Extended Assessment Procedures	
	Information Security Programs	
	Management Control Class	
	Operational Control Class	
	Technical Control Class	
	HIPAA: Agiliance 17799 HIGH_LEVEL Select All Clear All	
	04 - Risk assessment and treatment	
	05 - Security policy	=
	06 - Organization of information security	
	07 - Asset management	
	08 - Human resources security	
	09 - Physical and environmental security	
	10 - Communications and operations management	
	11 - Access control	
	12 - Information systems acquisition, development and maintenance	
	13 - Information security incident management	
	14 - Business continuity management	
	15 - Coppliance	×
Cancel	< Bac	k Next >

The Domain page.

- 8. Click **Select All** to choose all the domains related to a framework, or select specific domains that are applicable to one of the assessments. For example, to assess the security-related risks in your organization, you might choose the **Information Security Programs** domain.
- 9. Click **Next** to display.

Create New Controls by Co	ntent Wizard		×
1. Regulations	Step 4: Select Filters		* = required
2. Frameworks	You can filter controls and sub controls to work	on using one or more options.	
3. Domains 4. Filters	Vol can filter controls and sub controls to work     Control Types     Key Controls Only     Control organization     Make copy of controls (not recommended)     Merge multiple regulatory controls into a single tree     Keep redundant controls for reporting     Drop redundant controls	on using one or more options.     Subcontrol Types     All Subcontrols     CP level Subcontrols (Primary) only     No Subcontrols     Auto/Manual controls     Auto only     Manual only     Both	
Cancel		< Ba	ck Finish

The Filters page.

To match your business objective, you might want to run concise assessments by using various filters such as subcontrol types, control organization, auto/manual controls, and redundancy controls.

## 10. Click Finish.

Group: Information	Security Progra	ms							
	Group								
General Tags Applications	> Target En Prefe Owner Ar Group De	Title Information Security Programs Description The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization, wide information security program to address information security for the information and information security requires organizations to develop and implement an organization, including those provided or managed by another organization, contractor, The Information security requirements that support the operations and assets of the organization, including those provided or managed by another organization, contractor, The Information security requirements that are independent of any particular information system and are essential for managing information security programs. Organization-wide information security program to address escurity program plan supplements the individual security plans developed for each organization-wide information system. Together, the security plans or the individual information systems and the security plan for the information security program cover the totality of security controls employed by the organization. Target Entity's N/A Preferred Owner ship Author Agliance Group Details N/A Identifier N/A							
	New Contro	I Objective	New Questionnaire	New Control	More Ac	tions	*		Filter by All 💌
	🗌 Туре	Order	Title						
		1	PM-10 SECURITY A	UTHORIZATION	PROCESS				
		2	PM-09 RISK MANAG	SEMENT STRAT	EGY				
		3	PM-11 MISSION/BU	SINESS PROCES	S DEFINITIO	N			
		4	PM-06 INFORMATIC	IN SECURITY ME	ASURES OF	F PERFORMANC	Œ		
				ON SYSTEM INVE					