Select 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 Policy Manager.
- 2. Go to Policies > 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 cur	rently
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	ck 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 controls.				
3. Domains	(Framework choices marked by * are not currently installed at your site. Please contact Agiliano to purchase additional framework content.)				
4. Filters	FISMA Select All Clear All □ FISMA* □ NIST SP 800-53 (2009) HIPAA Select All Clear 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	k Next >			

The Frameworks page.

- 5. Click the checkbox next to all frameworks related to the regulations selected in the previous step.
- 6. 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 - Conniiance	×
Cancel	< Bac	k Next >

The Domain page.

- 7. 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.
- 8. Click **Next** to display.

Create New Controls by Co	ntent Wizard		X
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	Control Types	Subcontrol Types	
4. Filters	 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 	 All Subcontrols CP level Subcontrols (Primary) only No Subcontrols Auto/Manual controls Auto only Manual only Both 	
Cancel		< Ba	ick 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.

9. Click Finish.

Group: Information	Security Progra	ms							
	Group								
General Tags	Descri	otion The Fea informa organiz Append informa security informa	ation security for the info zation, contractor, or oth- dix F and focus on the o ation security programs. ty program plan suppleme	rmation and infor er source. The in ganization-wide Organizations do ents the individua	rmation systems that su nformation security prog to information security re ocument program manag al security plans develop	pport the operat ram management quirements that rement controls and for each org	tions and assets of the or nt (PM) controls describe are independent of any p in an organization-wide it	ganization, including the f in this Appendix, com articular information synthesis and formation security pro- rstem. Together, the s	mation security program to address nose provided or managed by anoth plement the security controls in ystem and are essential for managin ogram plan. The organization-wide ecurity plans or the individual organization.
Applications	Target Entity's N/A Preferred								
Applications	Ownership								
		rthor Agiliand	ice						
	Group De	tails N/A tifier N/A							
	Iden	Unier N/A							
	New Contro	I Objective	New Questionnaire	New Control	More Actions	~			Filter by 🛛 All 🛛 👻
	🗌 Туре	Order	▲ Title						
	•	1	PM-10 SECURITY AI	JTHORIZATION F	PROCESS				
		2	PM-09 RISK MANAG	EMENT STRATE	GY				
		3	PM-11 MISSION/BUS	INESS PROCESS	S DEFINITION				
	100				ASURES OF PERFORMA	NCE			
	a ,	4	PM-U6 INFORMATIO	A SECORITY MEX	ASURES OF PERFORING	ANCE.			