Selecting Domain-Specific Controls

Policy authors identify risks in different domains that significantly impact their organization. Creating a control using content wizard is a content action which provides the freedom to choose the 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:

- In the RiskVision application, go to Controls > Controls and Questionnaires, and select the desired controls group. In the RiskVision application, go to Risks > Controls and Questionnaires, and select the desired controls group. In the RiskVision application, go to Policies > Controls and Questionnaires, and select the desired controls group.
- 2. Select New Controls with Content Wizard in the Actions pull-down list to launch Create New Controls by Content Wizard, displaying the Regulations wizard page.

Create New Controls by	Content Wizard	×
1. Regulations	Step 1: Select Regulations	* = required
2. Frameworks	Start with the Regulations that impact your organization. (Choices marked by * are not currently	
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	< Back	Next >

3. Select one or more regulations and click Next. The Frameworks wizard page appears.

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 con	
3. Domains	(Framework choices marked by * are not currently installed at your site. Please contact Ag to purchase additional framework content.)	jillance Sales
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 >

4. Choose frameworks related to the regulations selected in the previous step and then click **Next**. The **Domains** wizard page appears.

Create New Controls by Co	ntent Wizard	×
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 - Compliance	~
Cancel	< Ba	ck Next >

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

Create New Controls by C	ontent Wizard		<mark>.</mark>
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		< B	ack Finish

- 6. To match the 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.
- 7. Click **Finish** to add domain-specific controls to create programs and assessments that assess your organization's risk with respect to the specified domains.

Content Pack: NISTpack >	📙 Group: NIS	T SP 800-53	3 (2009) > 🎳 Group: Information Security Programs	
Group: Information Se	curity Progra	ms		
General >		tion The Fe informa organiz Append informa securit	ation Security Programs ideral Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to a ation security for the information and information systems that support the operations and assets of the organization, including those provided or managed b zation, contractor, or other source. The information security program management (PM) controls described in this Appendix, complement the security control dix F and focus on the organization-wide information security requirements that are independent of any particular information security program management controls in an organization-wide information security program plan. The organization stion security programs. Organizations document program management controls in an organization-wide information security program plan. The organization by program plan supplements the individual security plans developed for each organizational information system. Together, the security plans or the individual stion systems and the security plan for the information security program cover the totatity of security controls employed by the organization.	oy anoth∈ Is in nanagini n-wide
Tags Applications	Group De	rred ship thor Agiliano tails N/A ifier N/A	New Questionnaire New Control More Actions	
	Type	Order 1 2 3 4		