

Callio Secura 17799

написано Александр Астахов | 11 июня, 2023

Компания Callio Technologies была основана в 2001 году двумя канадскими академиками и специализируется в области разработки программных продуктов для анализа информационных рисков и управления информационной безопасностью в соответствии с требованиями стандартов BS 7799 и ISO 17799. *Callio Secura 17799* представляет собой комплексную систему для разработки, внедрения, эксплуатации и сертификации Системы управления информационной безопасностью (СУИБ) на основе стандарта BS 7799.

Также разработчик предлагает инструментальный комплект Callio Toolkit Pro 17799, который представляет собой серию документов и утилит, объединенных с целью помочь в понимании стандарта и приведении СУИБ в соответствие с его базовыми требованиями.

Callio Secura 17799 предоставляет следующие основные возможности:

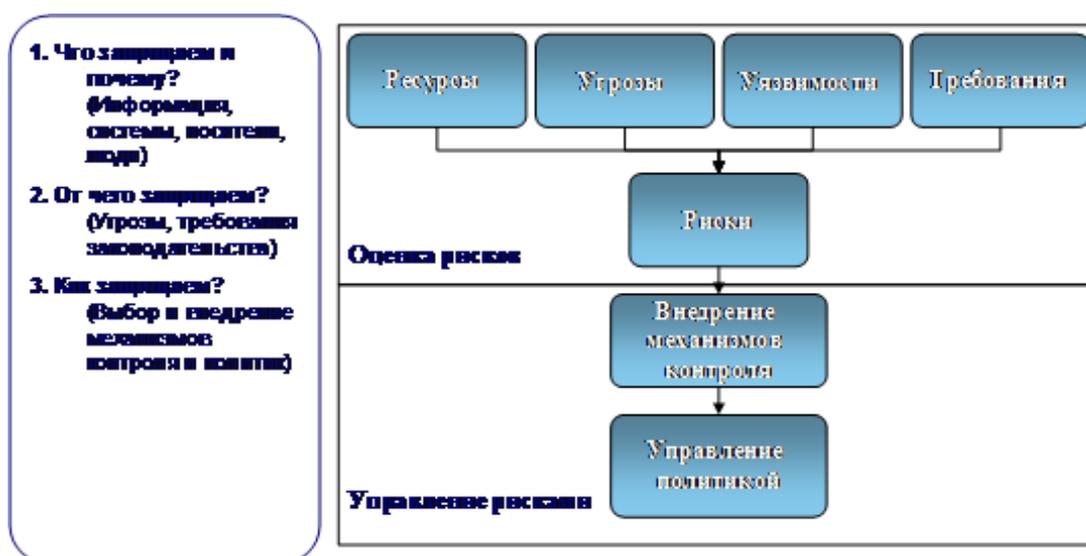
- оценку соответствия стандарту ISO 17799;
- инвентаризацию активов;
- описание структуры и процессов СУИБ;
- оценку и обработку рисков;
- разработку планов внедрения механизмов контроля;
- шаблоны политик безопасности (свыше 50 примеров);
- управление документами;
- управление опросными листами;
- оценку готовности к сертификации СУИБ по требованиям международного стандарта ISO 27001.

Процесс управления рисками по Callio состоит из двух этапов.

На первом этапе производится идентификация активов, угроз, уязвимостей и требований безопасности, оценивается величина уязвимостей, вероятность угроз и ценность активов. На

основании этих данных вычисляются значения рисков.

На втором этапе принимается решение относительно способов обработки рисков, приемлемого уровня остаточных рисков, разрабатывается план обработки рисков, производится внедрение механизмов контроля и разработка политик безопасности и других организационно-распорядительных документов.



Callio Secura 17799 предоставляет Web-интерфейс, механизмы коллективной работы, распределения ролей и полномочий между участниками процессов управления ИБ – рабочими группами, реализует управление документами, предоставляет шаблоны документов и опросники, а также методологию анализа и управления рисками. Система реализует рабочий процесс (workflow), который используется при внедрении СУИБ и подготовке к сертификации.

Процесс подготовки к сертификации начинается с первоначальной диагностики, в ходе которой выполняется оценка соответствия текущего состояния ИБ требованиям стандарта (gap analysis).

1. Заполнение опросника (127 вопросов) для оценки состояния системы управления безопасностью, на основе ежедневных контролей, процедур и политик, описанных в ISO 17799.
2. Изучение опросника из 127 ежедневных контролей, описанных в Стандарте, в соответствии с Руководством.
3. Идентификация существующих мер защиты. Проверка ежедневных контролей, которые были полностью или частично реализованы, являются неправильными, либо отсутствуют.

The screenshot shows a web browser window with the URL 'callio.secura.17799'. The page title is 'ABC ISMS [Change ISMS]'. The breadcrumb navigation is 'Home > Risk Assessment > Preliminary Diagnostic > Section Selection > Answers'. The main content area is titled 'Answers' and shows 'Section : 9.1 - Business requirement for access control' and '9.1.1 - Access control policy'. The 'Question' is: 'Are business requirements for access control defined and documented, and is access restricted to what is defined in the access control policy? [Guide]'. The 'Answer' is 'Partially'. The 'Justification' is: 'There is a policy already defined on ABC organisation, but it needs modification and'. The 'Reasons' are: '#1 Culture', '#2 Technology', and '#3 (To define)'. At the bottom, there are buttons for '<< Previous page', 'Return', and 'Next page >>'. The footer says '© 2003, Callio Technologies. All rights reserved'.

На следующем этапе производится оценка рисков. Процесс оценки рисков начинается с инвентаризации активов. Он включает в себя идентификацию и категорирование ресурсов, составление перечня сведений ограниченного распространения и реестра информационных активов.

The screenshot shows a web browser window with the URL 'callio.secura.17799'. The page title is 'ABC ISMS [Change ISMS]'. The breadcrumb navigation is 'Home > Risk Assessment > Asset-Context Integration'. The main content area is titled 'Asset-Context Integration'. There is a 'Context' dropdown menu with the value 'Development, testing and coding information'. Below it is an 'Add' button. The main content is a table titled 'List of Assets'.

Actions	Asset	Owner
	BPE, CCTV	Sam Dion
	Commodity, Air conditioning	No owner
	Commodity, Electricity supply	No owner
	Document, softwares manual	Sam Dion
	Hardware, AIX server	Sam Dion
	Hardware, CD- Rom Drives	Sam Dion
	Hardware, Hard drives	Sam Dion
	Hardware, Network cables	Elvis won
	Hardware, Network cards	Sam Dion
	Hardware, NT server	Sam Dion
	Hardware, Switch	Sam Dion
	Media, Backup tapes, CDs and disks	Elvis won

Далее для каждого актива оценивается его ценность для организации, которая определяется ущербом в результате

нарушения его конфиденциальности, целостности, доступности или невыполнения требований при осуществлении угроз безопасности.

1. Для каждого ресурса оценивается ущерб от нарушения безопасности или не выполнения требований законодательства. Используются количественная шкала: 1-3.
2. Назначается шкала оценки (например, 1-очень низкий, 2-низкий, 3-средний, 4-высокий, 5-очень высокий).
3. Проводится обоснование оценок для целей аудита.

Asset Evaluation - Value of the Asset

Context: Development, testing and coding information
Asset: Commodity, Air conditioning

Actions	Criterion	Value	Evaluation	Justification
	Confidentiality	(0) Not applicable		The confidentiality of the information won't be hurt if
	Integrity	(1) Low		information has a low impact if there's no air conditioning for
	Availability	(3) High		No airconditioning could result a disfunctioning of the servers
	Legal	(0) Not applicable		no legal impact

Save

© 2003, Callio Technologies. All rights reserved.

Идентификация рисков предполагает установку взаимосвязей между активами, уязвимостями и угрозами безопасности. Эта задача была бы очень непростой, т.к. для обычной организации таких взаимосвязей насчитывается несколько тысяч. Используемый инструментарий облегчает нам эту задачу, предлагая установки по умолчанию.

1. Идентификация уязвимостей, угроз, требований бизнеса и законодательства в их связи с ресурсами, используемыми для обработки критичной информации.
2. Используйте стандартные установки, предлагаемые Callio Secura 17799.

Identification of Threats

Context: Development, testing and coding information
Asset: Commodity, Air conditioning

Category: Business continuity

Threats: Legal requirement Business requirement

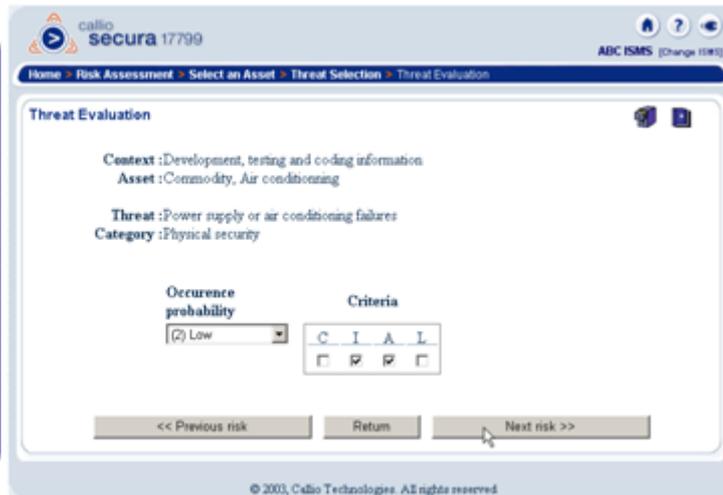
Actions	Suggested	Selected	Threat
		<input type="checkbox"/>	Interruption of business activities
	*	<input checked="" type="checkbox"/>	Lack of business continuity plan and procedures
		<input type="checkbox"/>	Lack of business continuity responsibilities, testing and training
	*	<input checked="" type="checkbox"/>	Natural and human disasters
		<input type="checkbox"/>	Unavailability of info, services and info processing facilities

Save

© 2003 Callio Technologies. All rights reserved.

Далее для вычисления рисков определяются вероятности реализации угроз. Для каждой угрозы указывается вид ущерба.

1. Используйте собственную вероятностную шкалу для каждой СУИБ.
2. Определите количественно вероятность реализации угроз, используя шкалы, идентифицированные для каждого ресурса уязвимости.
3. Определите с чем связан ущерб: нарушение конфиденциальности, целостности, доступности или нарушение требований законодательства.



Базируясь на информации о ценности активов и вероятности угроз, система автоматически вычисляет значения рисков и производит их упорядочивание по приоритетам.

1. Просмотр рисков в порядке приоритета.
2. Риск = ущерб х вероятность реализации угрозы или нарушения требований законодательства или бизнеса.
3. Просмотрите отчет об анализе рисков, чтобы принять правильное решение о том, что с ними делать (уменьшить, принять, избежать или перенести).



Когда оценка рисков завершена, можно переходить к выбору и внедрению механизмов контроля, необходимых для минимизации рисков. CallioSecurana основании результатов оценки рисков автоматически формирует набор рекомендуемых механизмов контроля из числа описанных в стандарте. Для каждого механизма контроля предоставляется его текущий статус.

По завершении этого этапа формируется план создания СУИБ. После этого можно переходить к разработке и внедрению политик безопасности.

1. На основании результатов анализа рисков Callio Secura 17799 предлагает различные стратегические, технические и физические механизмы контроля.
2. Выбор из предложенных механизмов контроля и обновление принятых решений по каждому механизму.
3. Чтобы правильно понимать смысл механизмов контроля, используйте руководства по внедрению, интерпретации рекомендательного стандарта, цели контроля, а также словарь терминов.

Domain Sections : 9 - Access control			
9.1 - Business requirement for access control			
No.	Control	Suggested	Status
9.1.1	Access control policy	Yes	Selected
9.2 - User access management			
No.	Control	Suggested	Status
9.2.1	User registration	Yes	Don't know
9.2.2	Privilege management	Yes	Selected
9.2.3	User password management	Yes	No selected
9.2.4	Review of user access rights	Yes	Incomplete
9.3 - User responsibilities			
No.	Control	Suggested	Status
9.3.1	Password use	Yes	Incomplete
9.3.2	Unattended user equipment	Yes	Incomplete

Для разработки политик безопасности используются шаблоны типовых документов. Базируясь на результатах анализа рисков, система автоматически формирует набор необходимых шаблонов. Готовые политики экспортируются в модуль управления документами, который позволяет производить их ревизию, согласование и публикацию на Web-портале.

1. Создание политик безопасности с использованием в качестве предоставленных Callio Secura 17799 (85 политик и более 500 различных положений ISO 17799).
2. На основании результатов анализа рисков автоматически формируется набор политик в модуле «Policy Generator».
3. Выберите, добавьте, удалите и измените набор политик.
4. Набор политик экспортируется в модуль «document manager» для согласования и публикации.

List of Policies			
Mod. No.	Description	Guideline No.	
1	Information security policy	6	
2	Information security infrastructure	18	
3	Security of third party access	12	
4	Outsourcing	9	
5	Accountability for assets	7	
6	Information classification	26	
7	Security in job definition and resourcing	29	
8	User training	7	

Всего имеется более 100 различных документов, которые используются при реализации механизмов контроля СУИБ. Если предложенных системой шаблонов недостаточно, мы можем выбрать дополнительные документы и экспортировать их в модуль управления документами.

1. Около 100 документов, включая шпаргалки, списки проверок, примеры, дополнительная информация и шаблоны и используются для реализации механизма контроля СУИБ в соответствии с ISO 17799.
2. Выберите нужные шаблоны и экспортируйте их в формате «document management».

No.	Standard section	Templates Suggested	Templates Available	Templates Selected	Templates Exported
3.1	Information security policy	*	6	0	0
4.1	Information security infrastructure	*	2	2	1
4.2	Security of third party access		0	0	0
4.3	Outsourcing		0	0	0
5.1	Accountability for assets		1	1	0
5.2	Information classification		3	0	0
6.1	Security in job definition and resourcing		13	13	13
6.2	User training		3	3	0
6.3	Responding to security incidents and malfunctions		6	0	0
7.1	Secure areas		11	0	0
7.2	Equipment security		8	0	0
7.3	General controls		1	0	0
8.1	Operational procedures and responsibilities	*	7	3	3
8.2	System planning and acceptance		0	0	0
8.3	Protection against malicious software		0	0	0
8.4	Housekeeping		3	0	0

После того как создание СУИБ завершено – люди обучены, политики разработаны и внедрены, а функционирование механизмов контроля подтверждается документированными свидетельствами, – производится диагностика СУИБ с целью определения степени ее готовности к сертификации. Для этого используются специальный опросник и сопроводительные инструкции, предоставляемые системой.

1. Проверьте что СУИБ готова к сертификации по BS 7799-2.
2. Ответьте на 81 вопрос, которые помогут проверить что СУИБ позволяет устанавливать, контролировать, проверять, сопровождать и сверять исключать существующую структуру управления.
3. Проверьте что в организации правильно осуществляется управление документацией и правильно распределены ответственность и обязанности.
4. Изучайте инструкции, интерпретирующие каждый вопрос.

Section : 1 - Establishing and managing the ISMS

No 1 (PD 3003 : 4.2.1.a.1 - Establish the ISMS - Scope of the ISMS)

Question: Is there a document that describes unambiguously the scope of the ISMS? [Guide]

Answer: Yes

Justification: created by caliso securia 17799 menu, and documented on the document management tool

Reasons: #1 [To define], #2 [To define], #3 [To define]

No 2 (PD 3003 : 4.2.1.a.2 - Establish the ISMS - Scope of the ISMS)

Question: Are significant exclusions from the scope identified and the reasons for these exclusions explained clearly? [Guide]

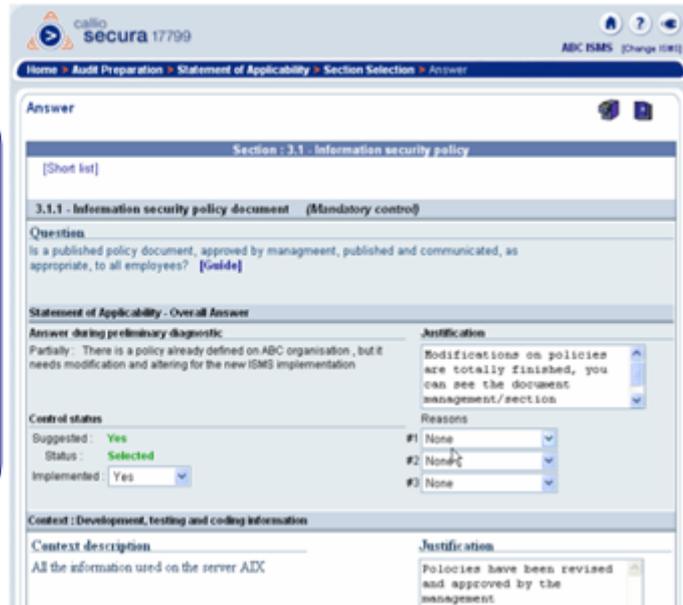
Answer: No

Justification: There is no exclusion on the scope for the moment

Reasons: #1 [To define]

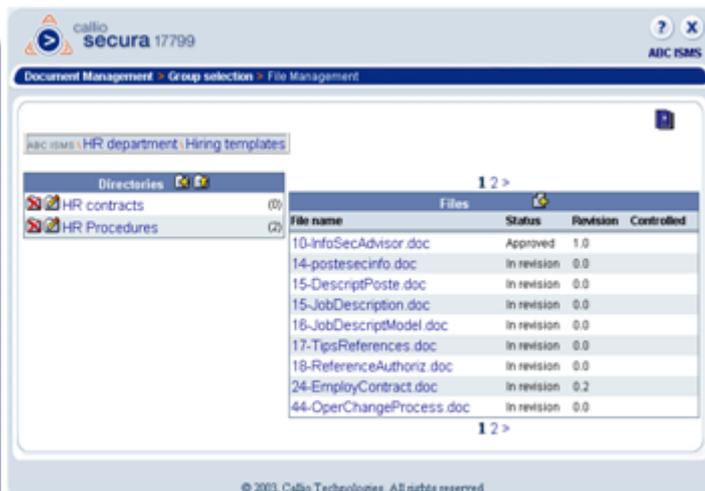
Декларация о применимости является последним разрабатываемым документом и обязательным условием для сертификации. В нем для каждого механизма контроля, описанного в стандарте, указывается его применимость, текущий статус, степень реализации и обоснование его использования. Это первый документ, который изучается аудиторами во время сертификации.

1. Документирование и обоснование применимости каждого из 127 элементов контроля.
2. Документирование состояния реализации каждого элемента для каждого ресурса.
3. Используйте руководство по аудиту для оценки эффективности реализации элементов контроля.
4. Сгенерируйте общее или детализированное Заключение о применимости и экспортируйте его в модуль «document manager».



В составе системы есть специальный модуль управления документами, который позволяет хранить все документы, имеющие отношение к функционированию СУИБ в центральной базе данных, публиковать и управлять доступом к этим документам для различных рабочих групп через веб-интерфейс. При помощи этого инструмента выполняются такие необходимые задачи, как согласование и утверждение документов, а также контроль версий.

1. Соберите файлы и документы, независимо от их формата, в центральной базе данных на Web сервере.
2. Предоставьте различным рабочим группам права доступа к документам и назначьте привилегии, такие как просмотр, печать, архивирование для каждой рабочей группы.
3. Управляйте контролем версий, создавая новые, утверждая и публикуя новые документы.
4. Проведите аудит и утвердите файлы для сертификации.



Callio Secura 17799 служит примером системы, которая объединяет функции управления рисками с функциями поддержки других процессов жизненного цикла СУИБ, таких как управление документами, контроль соответствия требованиям стандарта ISO 17799 и предсертификационный аудит СУИБ.