

# Test Module10.13

## Security Categories

### Test Cases

*Author(s): imbus AG  
MoReq2 test development team*

*Date: 16/04/2008*

*Version: 1.0*

*Status: Approved*

*Customer: Serco Consulting*

## Contents

Document History .....	3
<i>T10.13 Security Categories</i> .....	4
T10.13.1 Configuration .....	5
T10.13.1.1 Configuration of Options Concerning the Assignment of Security Categories .....	5
T10.13.1.2 Specifying User Roles with the Privilege to Specify and Change Security Categories .....	6
T10.13.1.3 Application of Default Clearance for New Users (Sub-Category is not Hierarchical) .....	7
T10.13.1.4 Assignment of Hierarchical Default Security Category Values .....	8
T10.13.1.5 Assignment of a Non-Hierarchical Sub-Category .....	9
T10.13.1.6 Actions when a Record with a Higher Security Category is Captured .....	10
T10.13.2 Management of Security Categories .....	11
T10.13.2.1 Creation of Security Categories with and without Sub-Categories .....	11
T10.13.2.2 Support of a Hierarchy of at least Five Levels .....	12
T10.13.2.3 Changing of the Security Category of Aggregations or Records .....	13
T10.13.2.4 Preventing an Aggregation from Having a Lower Security Category than any Record within it .....	14
T10.13.2.5 Changing of the Security Category of All Records in One Step .....	15
T10.13.3 Assignment of Security Categories to Aggregations and Records .....	16
T10.13.3.1 Automatic Assignment of a Default Value for a New Security (Sub-) Category .....	16
T10.13.3.2 Capture of a Record into a File with a Lower Security Category .....	17
T10.13.3.3 Notification to an Administrative Role if the Security Category of a Record is Lowered .....	18
T10.13.3.4 Simple Query to Determine the Highest Security Category .....	19
T10.13.3.5 Automatic Downgrade of a Security Category to the Lowest Level .....	20
T10.13.3.6 Automatic Downgrade of a Security Category to a Lower, Preselected Level .....	21
T10.13.3.7 Notification to an Administrative Role when Period for Security Category has Expired .....	22
T10.13.4 History and Audit Trail .....	23
T10.13.4.1 History of Security Category Values .....	23
T10.13.4.2 Entering a Reason Why the Security Category Value is Changed .....	24
T10.13.4.3 Logging of All Changes in the Audit Trail .....	25
T10.13.4.4 Information Recorded when Changing Security Category Values .....	26
T10.13.5 Assignment of Security Clearances to New Users .....	27
T10.13.5.1 Application of Most Restricted Clearance to a New User (Hierarchical Sub-Categories) .....	27
T10.13.5.2 Application of Different Security Clearances to Users in User Roles .....	28
T10.13.6 Controlling the Access to Aggregations and Records .....	29
T10.13.6.1 Restricted Access to Records .....	29
T10.13.6.2 Viewing Security Category Values and their History with Appropriate Security Clearance .....	31
T10.13.6.3 Application of Security Categories to Aggregations with no Access Permission .....	32
T10.13.7 Others .....	33
T10.13.7.1 Implementations of Complex or Unique Security Rules .....	33
T10.13.7.2 Review of Security Categories .....	34
T10.13.7.3 Controlled Vocabularies Limiting Allowable Values for Sub-Categories .....	35

## Document History

Version	Date of Issue	Author	Comment
0.1	05/11/08	Michael Sill	Initial Draft
0.2	12/11/08	Michael Sill	Revised after internal Review
0.3	19/11/08	Esther Kausz	Revision after receiving draft 5 of MoReq2
0.4	28/02/2008	Claudia Schieber	Revised after publishing of the final draft of the MoReq2 specification
1.0	02/04/2008	MoReq2 test development team	Finalising after approval of the test framework

**T10.13 Security Categories**

<b>REMARKS</b>	TEST DATA:	The test data for the following tests (test module 10, chapter T10.13) can be found in the corresponding test data repository. The reference chapter is called ' <b>on chapter T10.13 – Security Categories</b> '.
	TEST EXECUTION:	<p>step (1) Please read the chapter <b>Testframework – Introduction/Chapter 2</b> before starting the test execution.</p> <p>step (2) The test cases are designed in a way that enables you to skip certain test cases when required. However, the outcome of some test cases might be a precondition of subsequent tests. Where there are dependencies we have inserted test references into the precondition section of the test case. Careful attention should be given to the preconditions of the test cases.</p>

### T10.13.1 Configuration

Abstract: This chapter focuses on testing the configuration possibilities for the security categories of the ERMS.

#### T10.13.1.1 Configuration of Options Concerning the Assignment of Security Categories

I. Global test case information		
<i>test case id:</i>	T10.13.1.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role is logged in at configuration time. Ensure that this role can select between different options of how the ERMS assigns security categories to aggregations and records.	
<i>Req.-ID:</i>	10.13.1	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Configuration time</li> <li>Logged in as user of role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Check the options concerning the assignment of security categories.	The ERMS provides the following options: <ul style="list-style-type: none"> <li>security categories are assigned to classes, files, sub-files and/or volumes (and not to individual records)</li> <li>security categories are assigned to individual records (and not to classes, files, sub-files and/or volumes)</li> <li>security categories are assigned both to individual records and to classes, files, sub-files and or/volumes.</li> </ul>
2.	Select one of the given options.	One option is selected.
<i>c. postcondition(s)</i>		
The ERMS provides different options concerning the assignment of security categories: <ul style="list-style-type: none"> <li>security categories are assigned to classes, files, sub-files and/or volumes (and not to individual records)</li> <li>security categories are assigned to individual records (and not to classes, files, sub-files and/or volumes)</li> <li>security categories are assigned both to individual records and to classes, files, sub-files and or/volumes.</li> </ul> and an administrative role can select one option at configuration time.		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.1.2 Specifying User Roles with the Privilege to Specify and Change Security Categories

I. Global test case information		
<i>test case id:</i>	T10.13.1.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role is logged in at configuration time. Ensure that this role can specify which user roles have the privilege to specify and change security categories.	
<i>Req.-ID:</i>	10.13.2	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Configuration time</li> <li>Logged in as user of role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Specify that the user roles <b>SecurityReviewer</b> and <b>MarketingAdministrator</b> can specify and change security categories.	It is configured that the user roles <b>SecurityReviewer</b> and <b>MarketingAdministrator</b> can specify and change security categories.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows an administrative role to specify which user roles have the privilege to specify and change security categories.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

**T10.13.1.3 Application of Default Clearance for New Users (Sub-Category is not Hierarchical)**

I. Global test case information		
<i>test case id:</i>	T10.13.1.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role specifies how a clearance has to be assigned to a new user at configuration time. A check is made to confirm that at least two options are available and that a previously selected option can be changed.	
<i>Req.-ID:</i>	10.13.7	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• Configuration time</li> <li>• Logged in as user of role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Check the options concerning the assignment of clearances to new user.	The ERMS provides one of the following options: <ul style="list-style-type: none"> <li>• the ERMS must require a valid clearance to be entered for each new user.</li> <li>• the ERMS must apply a default clearance for new users.</li> </ul>
2.	Select the option: <ul style="list-style-type: none"> <li>• the ERMS must apply a default clearance for new users.</li> </ul>	The option is selected.
3.	Select the option: <ul style="list-style-type: none"> <li>• the ERMS must require a valid clearance to be entered for each new user</li> </ul>	The option can be changed.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS provides options concerning the assignment of clearances to new users at configuration time or later. The previously selected option can be changed.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.1.4 Assignment of Hierarchical Default Security Category Values

I. Global test case information		
<i>test case id:</i>	T10.13.1.4	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	<p>The ERMS provides the following options to assign hierarchical sub-categories to new aggregations and records:</p> <ul style="list-style-type: none"> <li>the ERMS applies a default value that is selected by an administrative role</li> <li>the ERMS uses the parent aggregation's value as a default</li> <li>the ERMS requires an administrative role to enter a value</li> </ul> <p>The options can be selected at configuration time or later.</p>	
<i>Req.-ID:</i>	10.13.10	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Logged in as user or role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Check the option concerning the assignment of a hierarchical sub-category to new classes, records etc. at configuration time or later.	<p>The ERMS provides the following options at configuration time or any later time.</p> <ul style="list-style-type: none"> <li>the ERMS applies a given default value</li> <li>the ERMS uses the parent aggregation's value as a default</li> <li>the ERMS requires an administrative role to enter a value</li> </ul>
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows an administrative role to select one of several modes of operation to assign a hierarchical sub-category to a new aggregation or record at configuration time or later.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature



### T10.13.1.5 Assignment of a Non-Hierarchical Sub-Category

I. Global test case information		
<i>test case id:</i>	T10.13.1.5	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	<p>The ERMS provides the following options to assign non-hierarchical sub-categories to new aggregations and records:</p> <ul style="list-style-type: none"> <li>the ERMS applies a given default value that is selected by an administrative role</li> <li>the ERMS uses the parent aggregation's value as a default</li> <li>the ERMS allows but does not require an administrative role to enter a value</li> </ul> <p>The options can be selected at configuration time or later.</p>	
<i>Req.-ID:</i>	10.13.11	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Logged in as user of role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Check the options concerning the assignment of a non-hierarchical sub-category to new classes, records etc. at configuration time or later.	<p>The ERMS provides the following options at configuration time or any later time.</p> <ul style="list-style-type: none"> <li>the ERMS applies a given default value</li> <li>the ERMS uses the parent aggregation's value as a default</li> <li>the ERMS allows but does not require an administrative role to enter a value</li> </ul>
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows an administrative role to select one of several modes of operations to assign a sub-category to a new aggregation or record at configuration time or later.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.1.6 Actions when a Record with a Higher Security Category is Captured

I. Global test case information		
<i>test case id:</i>	T10.13.1.6	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	An administrative role is logged in at configuration time. Ensure that this user role can configure different actions when a record is captured that has a higher security category than the aggregation into which it is being captured.	
<i>Req.-ID:</i>	10.13.15	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• Configuration time</li> <li>• Logged in as user role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Configure the actions of the ERMS when a record is captured that has a higher security category than the aggregation into which it is being captured.	The ERMS offers at least the following actions: <ul style="list-style-type: none"> <li>• the security category of the file is raised to that of the record</li> <li>• the user is denied permission to capture the record into the file</li> <li>• the record is automatically sent to a specified user for action</li> <li>• the user is invited to create a new file for the record</li> </ul>
2.	Select the action that the user is denied permission to capture the record into the file.	The selected option is configured.
<i>c. postcondition(s)</i>		
<p>The ERMS allows an administrative role to configure the actions taken by the ERMS when a record is captured that has a higher security category than the aggregation into which it is being captured. The following actions can be chosen:</p> <ul style="list-style-type: none"> <li>• the security category of the file is raised to that of the record</li> <li>• the user is denied permission to capture the record into the file</li> <li>• the record is automatically sent to a specified user for action</li> <li>• the user is invited to create a new file for the record</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

## T10.13.2 Management of Security Categories

Abstract: This chapter focuses on testing the management of the security categories in the ERMS.

### T10.13.2.1 Creation of Security Categories with and without Sub-Categories

I. Global test case information		
<i>test case id:</i>	T10.13.2.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	Ensure that an administrative role can create a security category with sub-categories and a security category with no sub-categories.	
<i>Req.-ID:</i>	10.13.3	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Logged in as user of role <b>CentralAdministrator</b></li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Create the main security category <b>Security Categories (SC01)</b> in <b>TestSecurityCategory1</b> with the following sub-categories: <ul style="list-style-type: none"> <li><b>Security Class</b></li> <li><b>Caveat</b></li> <li><b>Descriptor</b></li> </ul>	The main security category <b>Security Categories (SC01)</b> in <b>TestSecurityCategory1</b> is created with three sub-categories.
2.	Create the main security category <b>Security Categories2 (SC02)</b> in <b>TestSecurityCategory1</b> with no sub-categories.	The main security category <b>Security Categories2 (SC02)</b> in <b>TestSecurityCategory1</b> is created with no sub-categories.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows an administrative role to create a security category with sub-categories.</li> <li>The ERMS allows an administrative role to create a security category with no sub-categories.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.2.2 Support of a Hierarchy of at least Five Levels

I. Global test case information		
<i>test case id:</i>	T10.13.2.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	Ensure that an administrative role can add a hierarchy of five levels to a sub-category. Unrestricted access is given at the lowest level. Highly restricted access is given at the highest level.	
<i>Req.-ID:</i>	10.13.6	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• Logged in as user of role <b>CentralAdministrator</b></li> <li>• <b>TestSecurityCategory1</b> is created and the security category <b>Security Categories (SC01)</b> exists (see test case T10.13.2.1)</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Create a hierarchy of the following levels in the sub-category <b>Security Class (SC01/01)</b> of security category <b>Security Categories (SC01)</b> : <ul style="list-style-type: none"> <li>• Top Secret (highly restricted access)</li> <li>• Secret</li> <li>• Confidential</li> <li>• Restricted</li> <li>• Unclassified (unrestricted access)</li> </ul>	Five levels in hierachical order are created in the sub-category <b>Security Class (SC01)</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS allows an administrative role to create five levels in hierachical order in a sub-category.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.2.3 Changing of the Security Category of Aggregations or Records

I. Global test case information		
<i>test case id:</i>	T10.13.2.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	Ensure that an administrative role can change the security category of aggregations and of a record.	
<i>Req.-ID:</i>	10.13.17	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user of role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> <li>• The class <b>Human Resources (CS01/008)</b> and all aggregations and records below have the security category value <b>Unclassified</b> for the security category <b>SecurityCategory (SC01)</b>.</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Change the security category value of the class <b>Human Resources (CS01/008)</b> to <b>Restricted</b> .	The security category value of the class <b>Human Resources (CS01/008)</b> is changed.
2.	Change the security category value of the file <b>Employees (CS01/008/001)</b> to <b>Restricted</b> .	The security category value of the file <b>Employees (CS01/001/001)</b> is changed.
3.	Change the security category value of the sub-file <b>Outsourcing (CS01/008/001/001)</b> to <b>Restricted</b> .	The security category value of the sub-file <b>Outsourcing (CS01/008/001/001)</b> is changed.
4.	Change the security category value of the volume <b>CompanyA (CS01/008/001/001/001)</b> to <b>Restricted</b> .	The security category value of the volume <b>CompanyA (CS01/001/001/001/001)</b> is changed.
5.	Change the security category value of the record <b>Record8 (CS01/008/001/001/001/001)</b> to <b>Restricted</b> .	The security category value of the record <b>Record8 (CS01/001/001/01/001/001)</b> is changed.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS allows an administrative role to change the security categories of aggregations and records.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

## T10.13.2.4 Preventing an Aggregation from Having a Lower Security Category than any Record within it

I. Global test case information		
<i>test case id:</i>	T10.13.2.4	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input checked="" type="checkbox"/> Optional
<i>test case description:</i>	An administrative role attempts to assign a security category value to a class which is lower than the security category value assigned to a record below. A check is made to ensure that the ERMS prevents this assignment.	
<i>Req.-ID:</i>	10.13.14	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Attempt to assign the value <b>Confidential</b> of sub-category <b>Security Class</b> to the class <b>Sales (CS01/003)</b> .	The ERMS denies the attempt to assign the security category.
2.	Attempt to assign the value <b>Confidential</b> of sub-category <b>Security Class</b> to the file <b>Sales Policy (CS01/003/001)</b> .	The ERMS denies the attempt to assign the security category.
3.	Attempt to assign the value <b>Confidential</b> of sub-category <b>Security Class</b> to the sub-file <b>2007 (CS01/003/001/001)</b> .	The ERMS denies the attempt to assign the security category.
4.	Attempt to assign the value <b>Confidential</b> of sub-category <b>Security Class</b> to the volume <b>1<sup>st</sup> quarter (CS01/003/001/001/001)</b> .	The ERMS denies the attempt to assign the security category.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS prevents the assignment of a lower sub-category value to aggregations where a record within has a higher one.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.2.5 Changing of the Security Category of All Records in One Step

I. Global test case information		
<i>test case id:</i>	T10.13.2.5	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role selects a class. Ensure that this user role can change the security category of all records within this class in one step.	
<i>Req.-ID:</i>	10.13.27	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Select the class <b>Sales (CS01/003)</b> and change the security category value of all aggregations and records below to <b>Confidential</b> in one step.	All aggregations and records within the class <b>Sales (CS01/003)</b> get the security category value <b>Confidential</b> in one step.
2.	Select the file <b>Technical Infrastructure (CS01/009/001)</b> and change the security category value of all aggregations and records below to <b>Confidential</b> in one step.	All aggregations and records within the file <b>Technical Infrastructure (CS01/009/001)</b> get the security category value <b>Confidential</b> in one step.
3.	Select the sub-file <b>Phones (CS01/009/001/001)</b> and change the security category value of all aggregations and records below to <b>Restricted</b> in one step.	All aggregations and records within the sub-file <b>Phones (CS01/009/001/001)</b> get the security category value <b>Restricted</b> in one step.
4.	Select the volume <b>Wireless Communication (CS01/009/001/001/001)</b> and change the security category value of all aggregations and records below to <b>Unrestricted</b> in one step.	All aggregations and records within the volume <b>Wireless Communication (CS01/009/001/001/001)</b> get the security category value <b>Unrestricted</b> in one step.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS allows an administrative role to change the security category of all aggregations and records within a class in one step.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3 Assignment of Security Categories to Aggregations and Records

Abstract: This chapter focuses on testing the assignment of security categories to aggregations and records.

#### T10.13.3.1 Automatic Assignment of a Default Value for a New Security (Sub-) Category

I. Global test case information		
<i>test case id:</i>	T10.13.3.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role defines a new hierarchical security sub-category. A check is made to confirm that the most restricted value is assigned to all existing aggregations and records.	
<i>Req.-ID:</i>	10.13.12	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user in role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and aggregations</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Create a new security sub-category <b>Location (SC01/003)</b> with the values <b>Same Location, Same Country, Worldwide</b> .	The new security sub-category <b>Location</b> with the values <b>Same Location, Same Country and Worldwide</b> is created.
2.	Select the class <b>Marketing (CS01/001)</b> .	The most restricted value <b>Same Location</b> of sub-category <b>Location</b> is assigned.
3.	Select the file <b>Policy Development (CS01/001/001)</b> .	The most restricted value <b>Same Location</b> of sub-category <b>Location</b> is assigned.
4.	Select the sub-file <b>2006 (CS01/001/001/001)</b> .	The most restricted value <b>Same Location</b> of sub-category <b>Location</b> is assigned.
5.	Select the volume <b>1<sup>st</sup> quarter (CS01/001/001/001/001)</b> .	The most restricted value <b>Same Location</b> of sub-category <b>Location</b> is assigned.
6.	Select the record <b>Record1 (CS01/001/001/001/001/001)</b> .	The most restricted value <b>Same Location</b> of sub-category <b>Location</b> is assigned.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS applies the most restricted value of a new security (sub)category to all existing aggregations and/or records.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature



### T10.13.3.2 Capture of a Record into a File with a Lower Security Category

I. Global test case information		
<i>test case id:</i>	T10.13.3.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	The ERMS is configured to deny the user permission to capture a record that has a higher security category than the aggregation into which it is being captured. An administrative role captures a record in a file that has a higher security category than the aggregation into which it is being captured. Ensure that the ERMS takes the action configured at configuration time.	
<i>Req.-ID:</i>	10.13.15	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user or role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> <li>• The ERMS is configured to deny the user permission to capture a record if a record is captured that has a higher security category than the aggregation into which it is being captured (see test case T10.13.1.6).</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.	Attempt to capture the record <b>Record5</b> in the file <b>Management Planning (CS01/001/003)</b> and assign the value <b>Top Secret</b> of security sub category <b>Security Class</b> .	The ERMS denies the attempt to capture the record <b>Record5</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• If the ERMS is configured to take a special action when a record is captured that has a higher security category than the aggregation into which it is being captured, the ERMS takes the correct action.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3.3 Notification to an Administrative Role if the Security Category of a Record is Lowered

I. Global test case information		
<i>test case id:</i>	T10.13.3.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	A user role lowers the security category of a record. A check is made to ensure that an administrative role is notified and has to confirm the action before the operation can be completed.	
<i>Req.-ID:</i>	10.13.28	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user in role <b>MarketingAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Select the record <b>Record1 (CS01/001/001/001/001)</b> and lower the sub-category <b>SecurityClass</b> to <b>Unclassified</b> .	The change process of the security category of <b>Record1</b> is started.
2.	Log off user in role <b>MarketingAdministrator</b> .	User in role <b>MarketingAdministrator</b> is logged off.
3.	Log in user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged in.
4.	Check whether there is a notification about the change of the security category of <b>Record1</b> .	A notification about the change of the security category or <b>Record1</b> exists.
5.	Confirm the change of the security category of <b>Record1</b> .	The change of the security category of <b>Record1</b> is confirmed and the change is completed.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The administrative role is notified as soon as the security category of a record is lowered. Only after confirmation by the administrative role the operation can be completed.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3.4 Simple Query to Determine the Highest Security Category

I. Global test case information		
<i>test case id:</i>	T10.13.3.4	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	An administrative role determines the highest security category of a record in a class. A check is made to confirm that this can be done with one simple query.	
<i>Req.-ID:</i>	10.13.16	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user in role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.	Start a query in the class <b>Marketing (CS01/001)</b> to get the highest security category of any record below of this class.	A simple query is available to get the highest security category of any record below of the class <b>Marketing (CS01/001)</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS provides a simple query to determine the highest security category of any record in a class.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3.5 Automatic Downgrade of a Security Category to the Lowest Level

I. Global test case information		
<i>test case id:</i>	T10.13.3.5	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input checked="" type="checkbox"/> Optional
<i>test case description:</i>	An administrative role applies a security category to aggregations, which is only valid for a period of time and will be downgraded to the lowest level at the end of that period.	
<i>Req.-ID:</i>	10.13.22	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user or role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Select the class <b>Accounting (CS01/007)</b> and assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to the class <b>Accounting (CS01/007)</b> .
2.	Select all aggregations below of the class <b>Accounting (CS01/007)</b> and assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to all aggregations below of the class <b>Accounting (CS01/007)</b> .
3.	Set system time to current date + 2 days.	The system time is changed.
4.	Select the class <b>Accounting (CS01/007)</b> .	Check that the value of the sub-category <b>SecurityClass</b> was downgraded to <b>Unclassified</b> .
5.	Select all aggregations below of class <b>Accounting (CS01/007)</b> .	Check that the value of the sub-category <b>SecurityClass</b> was downgraded to <b>Unclassified</b> for all aggregations below of class <b>Accounting (CS01/007)</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS allows the allocation of security categories to aggregations, which are valid for a defined period of time and automatically downgrades the security category to the lowest level security category at the end of a defined period of time.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3.6 Automatic Downgrade of a Security Category to a Lower, Preselected Level

I. Global test case information		
<i>test case id:</i>	T10.13.3.6	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input checked="" type="checkbox"/> Optional
<i>test case description:</i>	An administrative role applies a security category to aggregations, which is only valid for a period of time and will be downgraded to a lower, preselected level at the end of that period.	
<i>Req.-ID:</i>	10.13.23	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user or role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Select the class <b>Infrastructure (CS01/004)</b> , assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day and define the value <b>Restricted</b> which should be assigned after that period.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to the class <b>Infrastructure (CS01/004)</b> . At the end of that period the value <b>Restricted</b> should be assigned.
2.	Select all aggregations below of the class <b>Infrastructure (CS01/004)</b> , assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day and define the value <b>Restricted</b> which should be assigned at the end of that period.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to all aggregations below of the class <b>Infrastructure (CS01/004)</b> . At the end of that period the value <b>Restricted</b> should be assigned.
3.	Set system time to current date + 2 days.	The system time is changed.
4.	Select the class <b>Infrastructure (CS01/004)</b> .	Check whether the value of the sub-category <b>SecurityClass</b> was downgraded to <b>Restricted</b> .
5.	Select all aggregations below of the class <b>Infrastructure (CS01/004)</b> .	Check whether the value of the sub-category <b>SecurityClass</b> was downgraded to <b>Restricted</b> for all aggregations below of class <b>Infrastructure (CS01/004)</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS automatically downgrades the security category of aggregations and records to a lower, preselected value at the end of a defined period of time.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
	<input type="checkbox"/> passed	
	<input type="checkbox"/> failed	
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.3.7 Notification to an Administrative Role when Period for Security Category has Expired

I. Global test case information		
<i>test case id:</i>	T10.13.3.7	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input checked="" type="checkbox"/> Optional
<i>test case description:</i>	An administrative role applies a security category value to aggregations and records, which is only valid for a period of time. A check is made to confirm that on expiry the administrative role is notified and he can both reassess and amend the security category value.	
<i>Req.-ID:</i>	10.13.24	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user in role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Select the class <b>Finance (CS01/005)</b> and assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to the class <b>Finance (CS01/005)</b> .
2.	Select all aggregations and records below of the class <b>Finance (CS01/005)</b> and assign the value <b>Confidential</b> of sub-category <b>SecurityClass</b> which should be valid for 1 day.	The sub-category <b>SecurityClass</b> with the value <b>Confidential</b> and validity of 1 day is assigned to all aggregations and records below of the class <b>Finance (CS01/005)</b> .
3.	Set system time to current date + 2 days.	The system time is changed.
4.	Check whether there is a notification about the expiry of the security category for the class <b>Finance (CS01/005)</b> .	A notification about the expiry of the defined period of time exists.
5.	Change the security category value to <b>Restricted</b> for the class <b>Finance (CS01/005)</b> and all its aggregations and records.	The ERMS allows changing the security category value for the class <b>Finance (CS01/005)</b> and all its aggregations and records.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS notifies the administrative role when the selected time period for a security category has expired. The administrative role can change the security category value.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.4 History and Audit Trail

Abstract: This chapter focuses on testing the audit trail and the history of the action taken concerning security categories.

#### T10.13.4.1 History of Security Category Values

I. Global test case information		
<i>test case id:</i>	T10.13.4.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role has changed the security values of aggregations and records. A check is made to confirm that the ERMS stores the old security category values in the metadata of the corresponding aggregations and records.	
<i>Req.-ID:</i>	10.13.19	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user in role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> <li>• The security category value of the class <b>Marketing (CS01/001)</b> has been changed (see test case T10.13.2.3)</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.	Open metadata of the class <b>Marketing (CS01/001)</b> and all its aggregations and records	The metadata holds the history about the old security category values.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS holds a history of security category values in the metadata of the records and aggregations to which they apply.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.4.2 Entering a Reason Why the Security Category Value is Changed

I. Global test case information		
<i>test case id:</i>	T10.13.4.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	An administrative role changes the value of a security category value. A check is made to confirm that <ul style="list-style-type: none"> <li>the administrative role can add a reason for the change</li> <li>the reason is stored with the history as metadata</li> </ul>	
<i>Req.-ID:</i>	10.13.20	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li><b>TestSecurityCategory1</b> is created</li> <li><b>TestClassificationScheme1</b> is created</li> <li>Logged in as user or role <b>CentralAdministrator</b></li> <li>The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Change the security category value of the class <b>Management (CS01/006)</b> to <b>Confidential</b> .	The ERMS allows entering a reason for the change.
2.	Enter a reason for the change and then open metadata of the class <b>Management (CS01/006)</b> .	The ERMS stores the entered reason in the history as metadata.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows entering a reason for the change of a security category value and stores the reason with the history as metadata.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature



### T10.13.4.3 Logging of All Changes in the Audit Trail

I. Global test case information		
<i>test case id:</i>	T10.13.4.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	The security category values of a class have been changed. Ensure that the ERMS logged all changes to the security category values in the audit trail.	
<i>Req.-ID:</i>	10.13.25	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user or role <b>CentralAdministrator</b></li> <li>• The ERMS supports security categories for both records and classes</li> <li>• Security category values of the class <b>Marketing (CS01/001)</b> were changed before (see test case T10.13.2.3)</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.	Open the audit trail.	The ERMS logged all changes to the security category and sub-category values in the audit trail.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS logs changes to security category and sub-category values in the audit trail.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.4.4 Information Recorded when Changing Security Category Values

I. Global test case information		
<i>test case id:</i>	T10.13.4.4	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	The ERMS logs at least the following information in the metadata of the corresponding aggregations or records when a security category value was changed: <ul style="list-style-type: none"> <li>• date</li> <li>• user</li> <li>• values before and after the change</li> <li>• reason</li> </ul>	
<i>Req.-ID:</i>	10.13.29	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user or role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> <li>• Security category values of the class <b>Marketing (CS01/001)</b> were changed before (see test case T10.13.2.3)</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Open the history of the class <b>Marketing (CS01/001)</b>	The ERMS logged at least the following details of the changes to the security categories in the metadata of the class <b>Marketing (CS01/001)</b> <ul style="list-style-type: none"> <li>• date</li> <li>• user</li> <li>• values before and after the change</li> <li>• reason</li> </ul>
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS logs details in the metadata of relevant aggregations or records when a security category value was changed.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.5 Assignment of Security Clearances to New Users

Abstract: This chapter focuses on testing the correct assignment of security clearances to new users.

#### T10.13.5.1 Application of Most Restricted Clearance to a New User (Hierarchical Sub-Categories)

I. Global test case information		
<i>test case id:</i>	T10.13.5.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role creates a new user. A check is made to confirm that the most restricted clearance of all security categories and sub-categories in the hierarchy is applied.	
<i>Req.-ID:</i>	10.13.8	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• Logged in as user of role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>check/ expected result</i>
1.	Create a new user <b>MA_username</b>	The most restricted clearance of all hierarchical security categories or sub-categories is applied to the new user <b>MA_username</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS assigns the most restricted clearance of hierarchical security categories and sub-categories to new users.</li> </ul>		
III. Test result		
<i>defects / deviations</i>	<i>verdict</i>	
	<input type="checkbox"/> passed <input type="checkbox"/> failed	
<i>Remarks</i>	<i>tester</i>	
	_____ date, signature	

## T10.13.5.2 Application of Different Security Clearances to Users in User Roles

I. Global test case information		
<i>test case id:</i>	T10.13.5.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	Ensure that an administrative role can apply a different security clearance to a user who inherited his security clearance from a role.	
<i>Req.-ID:</i>	10.13.13	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li><b>TestSecurityCategory1</b> is created</li> <li>Logged in as user or role <b>CentralAdministrator</b></li> <li>The ERMS supports the allocation of security clearances to roles which are then inherited to the users</li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Add the user <b>MA_username</b> to the user role <b>MarketingAdministrator</b> .	The user <b>MA_username</b> inherits the security clearance (security sub-category <b>SecurityClass</b> with value <b>Confidential</b> ) of its role <b>MarketingAdministrator</b> .
2.	Change the security clearance of <b>MA_username</b> to the value <b>Secret</b> of sub-category <b>SecurityClass</b> .	The ERMS allows to change the security clearance of a user who inherits his security clearance from a user role.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS allows security clearance to be allocated to a role and inherited by users.</li> <li>The ERMS allows to apply a different security clearance to users who inherited their former security clearance from the user role.</li> </ul>		
III. Test result		
<i>defects / deviations</i>	<i>verdict</i>	
	<input type="checkbox"/> passed <input type="checkbox"/> failed	
<i>Remarks</i>	<i>tester</i>	
	_____ date, signature	

## T10.13.6 Controlling the Access to Aggregations and Records

Abstract: This chapter focuses on testing mechanisms to control the access to aggregations and records.

### T10.13.6.1 Restricted Access to Records

I. Global test case information		
<i>test case id:</i>	T10.13.6.1	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	An administrative role changes the security clearance of a user to aggregations and records. A check is made to confirm that the user has only access to aggregations and records when his security clearance is equal or higher than the security category value of the aggregations and records.	
<i>Req.-ID:</i>	10.13.9	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user of role <b>CentralAdministrator</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Change the security clearance of user <b>MA_username</b> to the value <b>Confidential</b> of security sub-category <b>SecurityClass</b> .	The security clearance of user <b>MA_username</b> is changed.
2.	Change the security category value of the class <b>Marketing (CS01/001)</b> and all its aggregations and records to <b>Confidential</b> .	The class <b>Marketing (CS01/001)</b> and all its aggregations and records got a new sub-category value.
3.	Log off user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged off.
4.	Log in as user <b>MA_username</b> .	The user <b>MA_username</b> is logged in.
5.	Select the class <b>Marketing (CS01/001)</b> .	The user <b>MA_username</b> has access to the class <b>Marketing (CS01/001)</b> .
6.	Select the aggregations and records below of the class <b>Marketing (CS01/001)</b> .	The user <b>MA_username</b> has access to all aggregations and records below of the class <b>Marketing (CS01/001)</b> .
7.	Log off user <b>MA_username</b> .	The user <b>MA_username</b> is logged off.
8.	Log in as user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged in.
9.	Change the security clearance of user <b>MA_username</b> to the value <b>Secret</b> of security sub-category <b>SecurityClass</b> .	The security clearance of user <b>MA_username</b> is changed.
10.	Log off user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged off.
11.	Log in as user <b>MA_username</b> .	The user <b>MA_username</b> is logged in.
12.	Select the class <b>Marketing (CS01/001)</b> .	The user <b>MA_username</b> has access to the class <b>Marketing (CS01/001)</b> .
13.	Select the aggregations and records below of the class <b>Marketing (CS01/001)</b> .	The user <b>MA_username</b> has access to all aggregations and records below of the class <b>Marketing (CS01/001)</b> .
14.	Log off user <b>MA_username</b> .	The user <b>MA_username</b> is logged off.
15.	Log in as user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged in.
16.	Change the security clearance of user <b>MA_username</b> to the value <b>Unrestricted</b> of security sub-category <b>SecurityClass</b> .	The security clearance of user <b>MA_username</b> is changed.
17.	Log off user in role <b>CentralAdministrator</b> .	User in role <b>CentralAdministrator</b> is logged

		off.
18.	Log in as user <b>MA_username</b> .	The user <b>MA_username</b> is logged in.
19.	Attempt to select the class <b>Marketing (CS01/001)</b> .	The ERMS denies the attempt of user <b>MA_username</b> to access the class <b>Marketing (CS01/001)</b> .
20.	Attempt to select the aggregations and records below of the class <b>Marketing (CS01/001)</b> .	The ERMS denies the attempt of user <b>MA_username</b> to access the aggregations and records below of the class <b>Marketing (CS01/001)</b> .
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The ERMS restricts the access to aggregations and records if the user does not have either equal or higher security clearance than the security category value.</li> </ul>		
<b>III. Test result</b>		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed <input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.6.2 Viewing Security Category Values and their History with Appropriate Security Clearance

I. Global test case information		
<i>test case id:</i>	T10.13.6.2	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional
<i>test case description:</i>	A user with appropriate security clearance checks the current value of security category values and their history.	
<i>Req.-ID:</i>	10.13.21	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user <b>MA_username2</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.	Select the class <b>Acquisition (CS01/002)</b> .	The class <b>Acquisition (CS01/002)</b> is selected. The following information about the class <b>Acquisition (CS01/002)</b> can be seen: <ul style="list-style-type: none"> <li>• current value of the sub-categories</li> <li>• the history of the sub-categories</li> </ul>
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS allows users with appropriate security clearance to see both the current values of security categories and their history.</li> </ul>		
III. Test result		
<i>defects / deviations</i>	<i>verdict</i>	
	<input type="checkbox"/> passed <input type="checkbox"/> failed	
<i>Remarks</i>	<i>tester</i>	
	_____ date, signature	

### T10.13.6.3 Application of Security Categories to Aggregations with no Access Permission

I. Global test case information		
<i>test case id:</i>	T10.13.6.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	A user without appropriate security clearance attempts to apply a security category to an aggregation. A check is made to confirm that the ERMS prevents the application of the security category.	
<i>Req.-ID:</i>	10.13.26	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>• <b>TestSecurityCategory1</b> is created</li> <li>• <b>TestClassificationScheme1</b> is created</li> <li>• Logged in as user <b>MA_username3</b></li> <li>• The ERMS is configured to support security categories for both records and classes</li> </ul>		
<i>b. test steps</i>		
step	action/operation	Check/ expected result
1.	Attempt to apply a security category value of security sub-category <b>SecurityClass</b> to the class <b>Marketing (CS01/001)</b> .	The ERMS denies the attempt to apply the security sub-category value.
2.	Attempt to apply a security category value of security sub-category <b>SecurityClass</b> to the aggregations below of <b>Marketing (CS01/001)</b> .	The ERMS denies the attempt to apply the security sub-category value.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>• The ERMS does not allow a user to apply a security category to an aggregation that the user does not have access to.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature



### T10.13.7 Others

Abstract: This chapter focuses on testing various aspects of security categories that have not been tested in previous chapters.

#### T10.13.7.1 Implementations of Complex or Unique Security Rules

I. Global test case information		
<i>test case id:</i>	T10.13.7.1	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input checked="" type="checkbox"/> Not Testable
<i>test case description:</i>	The corresponding requirement is not testable.	
<i>Req.-ID:</i>	10.13.5	
II. Test case		
<i>a. precondition(s)</i>		
•		
<i>b. test steps</i>		
<i>step</i>	<i>action/operation</i>	<i>Check/ expected result</i>
1.		
<i>c. postcondition(s)</i>		
•		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.7.2 Review of Security Categories

I. Global test case information		
<i>test case id:</i>	T10.13.7.2	
<i>test case priority:</i>	<input type="checkbox"/> Mandatory	<input checked="" type="checkbox"/> Optional
<i>test case description:</i>	The documentation of the ERMS is checked to ensure that the ERMS supports routine, periodic, scheduled review of security categories.	
<i>Req.-ID:</i>	10.13.18	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Documentation of the ERMS is available</li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Check the documentation of the ERMS to ensure that the ERMS supports routine, periodic, scheduled review of security categories.	The ERMS supports routine, periodic, scheduled review of security categories, where a review consists of: <ul style="list-style-type: none"> <li>allowing a user (with appropriate clearance and permissions) to view specified records and their security categories;</li> <li>allowing the user to change the security categories</li> </ul>
<i>c. postcondition(s)</i>		
The ERMS supports routine, periodic, scheduled review of security categories, where a review consists of: <ul style="list-style-type: none"> <li>allowing a user (with appropriate clearance and permissions) to view specified records and their security categories;</li> <li>allowing the user to change the security categories.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature

### T10.13.7.3 Controlled Vocabularies Limiting Allowable Values for Sub-Categories

I. Global test case information		
<i>test case id:</i>	T10.13.7.3	
<i>test case priority:</i>	<input checked="" type="checkbox"/> Mandatory	<input type="checkbox"/> Optional <input type="checkbox"/> Not Testable
<i>test case description:</i>	The documentation of the ERMS is checked to ensure that the ERMS requires controlled vocabularies to be defined and maintained by an administrative role, which limit the allowable values for sub-categories.	
<i>Req.-ID:</i>	10.13.4	
II. Test case		
<i>a. precondition(s)</i>		
<ul style="list-style-type: none"> <li>Documentation of the ERMS is available</li> </ul>		
<i>b. test steps</i>		
step	action/operation	check/ expected result
1.	Check the chapter of the documentation of the ERMS that describes the values for sub-categories.	The documentation of the ERMS tells that the ERMS requires controlled vocabularies to be defined and maintained by an administrative role, which limit the allowable values for sub-categories.
<i>c. postcondition(s)</i>		
<ul style="list-style-type: none"> <li>The documentation of the ERMS tells that the ERMS requires controlled vocabularies to be defined and maintained by an administrative role, these vocabularies limiting the allowable values for each sub-category.</li> </ul>		
III. Test result		
<i>defects / deviations</i>		<i>verdict</i>
		<input type="checkbox"/> passed
		<input type="checkbox"/> failed
<i>Remarks</i>		<i>tester</i>
		_____ date, signature