



# Functional Design for CCMS Data Exchanges Appendix J—CCMS Data Exchange Non-functional Requirements

---

MARCH 2011



ADMINISTRATIVE OFFICE  
OF THE COURTS

---

INFORMATION SERVICES DIVISION

Judicial Council of California  
Administrative Office of the Courts  
Information Services Division  
455 Golden Gate Avenue  
San Francisco, California 94102-3688  
415-865-4200  
*www.courtinfo.ca.gov*

Copyright © 2011 by Judicial Council of California/Administrative Office of the Courts. All rights reserved.

Except as permitted under the Copyright Act of 1976 and as otherwise expressly provided herein, no part of this publication may be reproduced in any form or by any means, electronic or mechanical, including the use of information storage and retrieval systems, without permission in writing from the copyright holder. Permission is hereby granted to nonprofit institutions to reproduce and distribute this publication for educational purposes if the copies credit the copyright holder.

## Contents

1.0	CCMS Data Exchange Non-functional Requirements.....	1
1.1	Auditing Requirements.....	1
1.2	Logging Requirements.....	2
1.3	Monitoring Requirements.....	3
1.4	Scalability Requirements.....	4
1.5	Security Requirements.....	4

## Tables

Table 1. Auditing Requirements .....	2
Table 2. Logging Requirements .....	3
Table 3. Monitoring Requirements .....	3
Table 4. Scalability Requirements .....	4
Table 5. Security Requirements .....	4

## 1.0 CCMS Data Exchange Non-functional Requirements

This appendix details the non-functional requirements common across all data exchanges. Any non-functional requirements identified for specific data exchanges are documented in the respective data exchange in Section 4 “*Data Exchange Requirements and Design.*”

### 1.1 Auditing Requirements

Requirement	Requirement Details
CCMS.DX.N.Audit.Integration.1	<p>The system should maintain a record of the following data exchange lifecycle activities for accountability, reconstruction of events, and problem identification:</p> <ul style="list-style-type: none"> <li>▪ Request received</li> <li>▪ Request sent</li> <li>▪ Request delivered</li> <li>▪ Request not delivered</li> <li>▪ Request pending for replay</li> <li>▪ Request for replay failed</li> <li>▪ Response received</li> <li>▪ Response not received</li> <li>▪ Response sent</li> <li>▪ Response delivered</li> <li>▪ Received acknowledgement</li> <li>▪ Sent acknowledgement</li> </ul>
CCMS.DX.N.Audit.Integration.2	<p>The system should record the following attributes for each lifecycle activity to provide the current status of a transaction:</p> <ul style="list-style-type: none"> <li>▪ Type of event</li> <li>▪ Date and time</li> <li>▪ Source system or user name</li> <li>▪ Interface name</li> <li>▪ Message identifier</li> <li>▪ Transaction identifier (correlation identifier—one transaction may involve more than one messages)</li> <li>▪ Target system</li> <li>▪ Audit message</li> </ul>
CCMS.DX.N.Audit.Integration.3	<p>The system should protect the audit information from unauthorized access.</p>

Requirement	Requirement Details
CCMS.DX.N.Audit.Integration.4	The system should provide search capability to view the audit information by source system, target system, date and time, or other defined set of parameters.
CCMS.DX.N.Audit.Integration.5	The system should maintain audit information for a configurable period of time.
CCMS.DX.N.Audit.Integration.6	The system should store information at the Integrated Service Backbone (ISB), California Courts Technology Center (CCTC), or court/county level.

*Table 1. Auditing Requirements*

## 1.2 Logging Requirements

Requirement	Requirement Details
CCMS.DX.N.Logging.Integration.1	The system should maintain a log of event and activity information for technical troubleshooting and problem identification purposes.
CCMS.DX.N.Logging.Integration.2	The system should maintain a log for the following events and activities: <ul style="list-style-type: none"> <li>▪ Authentication success or failure</li> <li>▪ Authorization success or failure</li> <li>▪ Validation success or failure</li> <li>▪ Transformation success or failure</li> <li>▪ Mapping success or failure</li> <li>▪ Look-up success or failure</li> <li>▪ Routing success or failure</li> <li>▪ Message out of sequence error</li> <li>▪ Database connection success or failure</li> <li>▪ Communication failure, (e.g., database connectivity, Web Service connectivity, FTP connectivity)</li> </ul>

Requirement	Requirement Details
CCMS.DX.N.Logging.Integration.3	The system should record the following attributes for logging events: <ul style="list-style-type: none"> <li>▪ Type of event</li> <li>▪ Date and time</li> <li>▪ Source system or user name</li> <li>▪ Interface name</li> <li>▪ Log message</li> <li>▪ Log level</li> </ul>
CCMS.DX.N.Logging.Integration.4	The system should protect log information from unauthorized access.
CCMS.DX.N.Logging.Integration.5	The system should maintain log information for a configurable time period
CCMS.DX.N.Logging.Integration.6	The system should store information at the ISB, CCTC, or court/county) level.

*Table 2. Logging Requirements*

### 1.3 Monitoring Requirements

Requirement	Requirement Details
CCMS.DX.N.Monitoring.Integration.1	The system should communicate to the source system whether the message is delivered successfully.
CCMS.DX.N.Monitoring.Integration.2	The system should send message identifier, status, status description, and destination name information as part of the notification message.
CCMS.DX.N.Monitoring.Integration.3	The system should maintain record of notification sent to the source or target systems.

*Table 3. Monitoring Requirements*

## 1.4 Scalability Requirements

Requirement	Requirement Details
CCMS.DX.N.Scalability.Integration.1	The system should support scalability in following dimensions: <ul style="list-style-type: none"> <li>• Load scalability—ability to handle increased load by increasing the resource pool and not changing the data exchange design.</li> <li>• Geographic scalability—ability to maintain performance, usability regardless of expansion from concentration in a local area to a more distributed geographic locations.</li> <li>• Administrative scalability—ability for an increasing number of organizations to easily share a single distributed system.</li> </ul>

Table 4. Scalability Requirements

## 1.5 Security Requirements

Requirement	Requirement Details
CCMS.DX.N.Security.Integration.1	The system should provide a mechanism to authenticate users or systems involved in a data exchange.
CCMS.DX.N.Security.Integration.2	The system should provide a mechanism that encrypts and decrypts data of all incoming/outgoing messages.
CCMS.DX.N.Security.Integration.3	The system should provide the Dynamic Data Classification (DDC) to filter sensitive fields from being sent to the integration partners that are not entitled to receive the data.

Table 5. Security Requirements