

The following is an annotation of NAVA's Standards with regard to Document Management practices used in the annuity sales transaction. In the annotations, assignment of responsibility is established along with key points, which should assist those charged with implementing the Standards.

71.1	Any document used in the process shall be maintained in the Document Management Repository established for that purpose by the party having the principle interaction with the customer through the course of the STP Standards Transaction ("Transaction"). This includes all versions and 'working papers' pertinent to the Transaction.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • Electronic documents ("E-Documents") operate two ways relative to transaction processing within the STP Standards process. <ul style="list-style-type: none"> ○ The first is an "Active" state and the second is an "Inactive" state. ○ In the Active state, the document is intended to be a collaborative resource where authorized parties and applications can freely gain access to the document, within the limitations of assigned authorities (or, "permissions"), and are allowed to modify the content or structure of the document; again, assuming they have the authority to do so. ○ Once the transaction has the document in its in-active state, it is moved into Records Management as a legal record of the transaction. This is a greatly restricted state that is not intended to be collaborative. The Operational Standards below describe the state of the document; i.e., its collaborative state. While this is a substantially less restricted state than Records Management, it nonetheless is generally governed by the essential principles of document management.
71.2	Documents placed into the Document Management Repository shall be available to the applications and personnel authorized (i.e.; granted permissions) for such access by the principle parties in the Transaction.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • This includes access to forms libraries or other libraries maintained by the Insurer for documents needed by the Distributor to conduct a sales transaction. • The Distributor must allow the Insurer or any legal agency conducting an audit of the Insurer or of Insurer transactions access to documents

	<p>created and / or used in the conduct of the transaction.</p> <ul style="list-style-type: none"> • The Document Management System (DMS) governing the Repository has to offer all of the safe-guard functions normally associated with a document management system, eg; <ul style="list-style-type: none"> ○ Versioning must occur any time a document is “checked-in” ○ Security should operate at the document level ○ Full ‘logging’ of any and all activity in the DMS.
71.3	<p>Documents held in the Document Management Repository shall immediately comply with any "legal holds" issued by either of the principle parties in the Transaction.</p>
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • Any document(s) placed under ‘legal hold’ must be marked as such according to the policies and practices of the party having custody of the document(s). • Legal hold requests from one party must be honored by the other. • Physical transfer (electronic or paper) of legal hold documents must be provided by each party at the request of the other so long as the document falls within the NAVA Standards’ definition of documents or transaction related material.
71.4	<p>Auditable logs of all activity accessing and/or using the Document Management System shall be maintained and preserved until the Document is removed from the Document Management System and placed into Records Management.</p>
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • Any and all access to documents or other information held in the document management system set-up by the Distributor to hold documents created and / or used in the conduct of the transaction must be kept in a log indicating whether: <ul style="list-style-type: none"> ○ The document was read only. ○ The document was “checked-out” and, if so, “checked-in” ○ Any changes to the security initially assigned to the document

71.5	The function that moves the Document from Document Management to Records Management shall be the result of a 'release' instruction issued by the STP workflow.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • No document should be moved or 'state changed' from DMS to RMS (Records Management System) until it is in its final state; ie, complete and 'locked' (see <u>NAVA Standards 2006-61: e-Forms Locking and Binding</u>)
71.6	Documents managed by the Document Management System shall be governed by the general rules of 'check-out' and 'check-in' whereby the Document can be 'locked' by an application or user with the proper permission (authority) to do so from access by others until such time that the document has been "checked-in" or returned back to open status within the Document Management System.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • Any document being updated should be 'checked-out' thus insuring that other changes are made to the document during the update. • Any and all updates and / or other changes must be recorded into the auditable log of the DMS.
71.7	Documents may not be physically deleted from the Document Management System by any user or application except by the System's Administrator. Any such deletions will be recorded in the audit records prescribed in this set of Standards.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • While authorized users and / or applications can 'delete' a document or other information object (logs, etc), no user level operator of the DMS whether that is a person or an application should have the ability to permanently remove any document or other information object including the DMS log. • Only the DMS administrator should have the ability to permanently delete documents and / or information objects and, then, only within the scope of a formally instituted procedure governing the final termination of documents and / or information objects.

71.8	Documents may be logically deleted by any party having such authority granted by the document owner.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • No document or other information object can be deleted unless the author or, if there is not designated 'author,' the owner of that document has allowed that in the security attributes associated with the document (also known as, "permissions")
71.9	Any changes to Documents managed by the Document Management System will be reflected in 'Versions' of the iteration being changed. There will be as many versions as there have been changes made to the document with no limitation. Versioning activity will be reflected in the Audit logs prescribed in this set of Standards.
	<p>Responsibility assigned to Distributor and Insurer.</p> <ul style="list-style-type: none"> • Document Management conforming to NAVA's Standards will provide for document 'versioning.' • A document or other stored information object will have its version level elevated if there have been any changes made to that document or stored information object. • Versioning protocol (eg, whether version is single, double, or 'n' decimal positions) is allowed to conform to the standards protocol and policies of the party managing the document or information object. <ul style="list-style-type: none"> Eg; <ul style="list-style-type: none"> ○ Single: Version X.X ○ Double: Version X.X.X • If there is no established protocol or policy then a basic single decimal increment should be applied. <ul style="list-style-type: none"> ○ Eg, Version X.X
71.10	System requests for documents from the Distributor's Document Management System will be made using the data messages for accessing repositories and databases in accordance with NAVA Standards 2006-81 for Data Messages.
	Responsibility assigned to Distributor and Insurer.

	<ul style="list-style-type: none"> • NAVA Standards allow for document to be electronically accessed for verification and / or retrieval purposes through use of standard messaging protocols established in NAVA Standards 2006-81: Data Messages. • If documents are retrieved, they can only be “copied” and not “moved” from the original library.
--	--

CROSS REFERENCES	
<u>REFERENCE</u>	<u>SOURCE LOCATION</u>
STP Process Model Reference Links <ul style="list-style-type: none"> ❖ Account Opening ❖ Product Presentation ❖ Selection and Order Entry ❖ Principal Suitability Review ❖ Application Process ❖ Insurer Application Process 	
Related Documents	NAVA Position Paper on Documents and Records Management SEC Regulation 17a-4 NASD 3110 - Books and Records STP Glossary of Terms
Check lists	Check List for Implementation
STP Standards	All STP Standards