If you are using Confluence and Comala Document Management within an FDA regulated environment, then you might need to setup Confluence in accordance with the FDA CFR 21 part 11 regulation (link to: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cf/cfr/CFRSearch.cfm?CFRPart=11). This article provides an overview on how companies are using these tools to achieve compliance, and draws directly from the real life experience of our customers.

In this article we assume that Confluence is installed as a ‘closed system’. ‘Closed system’ is a regulatory term and refers to a situation where the access to the system is controlled by you. This would be the typical scenario within the corporate world, and hence was used here as a key assumption.

For our purposes, the CFR 21 part 11 covers two areas:

1. Electronic Records: This area relates to the data which is stored and managed within the system, i.e.: your Confluence pages. It imposes requirements on the system to ensure the electronic data can be used in lieu of paper documents (Subpart B).
2. Electronic Signatures: This area relates to how people can electronically sign documents and forms (i.e. Confluence pages), with the purpose that these electronic signatures substitute paper signature (aka ‘wet signatures’) (Subpart C)

This article covers both these areas and focuses on how Comala Document Management contributes to achieving compliance.

For an organization to be in compliance, the right tools must be paired with the appropriate quality processes. We outline these in the compliance table below.

A word of caution: the content and information you keep in Confluence, and how it is used within your quality management system, will have an impact on your compliance strategy. We highly recommend that you seek specific advice from a regulatory expert in regards to the optimal setup for your organization.

### 1. The Toolset Required to Set-up a Compliant Document Management System in Confluence

The following table shows what tools are needed to create a compliant configuration:

<table>
<thead>
<tr>
<th>Component</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confluence</td>
<td>The platform for creating, storing and using the electronic records.</td>
</tr>
<tr>
<td>Comala Document Management</td>
<td>A Comalatech app for Confluence which provides a way to enforce an approval process for documents. This approval process is supported by built-in electronic signatures and an audit log. The flexibility provided by Comala Document Management macro language enables configuring an approval process which reflects your defined documented approval processes and the different organisational roles you have.</td>
</tr>
<tr>
<td>Comala Publishing (optional)</td>
<td>A Comalatech app for Confluence which separates approved pages from pages which are still in the authoring and approval process. It creates a structure of an authoring space, where approved documents are automatically published into an official space. This helps ensure that users of documents will always access to the current approved release. It complements the functionality of Comala Document Management and is optional. Some customers find it easier to work with a set of two spaces, or it can be used in cases where there are more strict auditing requirements.</td>
</tr>
</tbody>
</table>

Comalatech does not claim compliance or certification of any of our tools, as it is not possible for any vendor to offer a compliant system. In addition to taking advantage of technical elements, compliant systems must also implement the necessary procedural and administrative controls.
**Secure infrastructure**

<table>
<thead>
<tr>
<th>Provide a secure platform where only authorized users are accessing and modifying the data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup facilities.</td>
</tr>
</tbody>
</table>

**Third-party User Management/Directory Solution**

<table>
<thead>
<tr>
<th>A directory service, or a single sign-on integrated with Confluence, to support user account management. Although not strictly required by the regulation, in most cases organizations in the regulated space seek more advanced security and authentication features which are not provided by Confluence's internal directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In particular, for the CFR 21 part 11, a common practice is to enforce periodic renewal of passwords. This feature requires a solution outside of Confluence.</td>
</tr>
</tbody>
</table>

## 2. A Compliance Checklist Against the FDA CFR 21 part 11

### Subpart B - Electronic Records

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement (the original wording is given in italics)</th>
<th>How to Achieve Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10 (a)</td>
<td>Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</td>
<td>Comalatech Apps Confluence Processes and Activities</td>
</tr>
<tr>
<td>11.10 (b)</td>
<td>The ability to generate accurate and complete copies of records in both human-readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</td>
<td>The Comala Document Management app provides an activity report for approved pages, with all historic review and approval activities (including signatures information) Confluence pages may be exported to PDF and MS-Word. The built-in PDF export may be upgraded with 3rd party apps to provide more comprehensive page metadata in the exported page. Define your preferred method for exporting data from Confluence, and verify this data consists of all the required elements.</td>
</tr>
<tr>
<td>11.10 (c)</td>
<td>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</td>
<td>Put in place a backup policy. Keep backups for the duration required by your records retention policies. The recommended backup also includes database backup (and not solely an XML backup), as this is the only backup which contains the historic data of page approvals and the Confluence audit trail.</td>
</tr>
<tr>
<td>11.10 (d)</td>
<td>Limiting system access to authorized individuals.</td>
<td>Comalatech apply all Confluence access restrictions and authorization. Confluence allows for the definition of users and groups, and content access control can be based on those groups. In order to enforce the more restrictive policies indicated in Subpart C, the Customer may need to rely on an external User Management/Directory Solution, such as Atlassian Crowd or Active Directory.</td>
</tr>
</tbody>
</table>
| 11.10 (e) | Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | Comala Document Management, through the Activity Report, provides a historic audit trail of approvals and electronic signatures. Each modification to a Confluence page is kept as a new (unofficial) version. It can be compared to any other version to show the modifications. | Comfluence needs to be configured and used in a way which supports this requirement:  
1. Pages are never deleted but are retired and kept in the system (so that the history is retained).  
2. Official versions of pages need to be managed.  
3. Backup of the database, to ensure that the approval audit trail and electronic signature information is retained.  
4. Pages do not contain data which is modified in an uncontrolled manner: i.e. JIRA reports gadget which is dynamic by nature. |
| 11.10 (f) | Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | The Comala Document Management macro language provides control mechanisms to support a wide range of business rules. | Configure Comala Document Management to reflect your defined approval process. |
| 11.10 (g) | Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | Comala Document Management verifies the user has the necessary authority to perform key functions, and supports role-based and electronically signed approvals. | refer to 11.10(d) refer to 11.10(d) |
| 11.10 (h) | Compliant Electronic Document Management Systems must use device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | Not applicable | Not applicable - the source of data is not a device. |
| 11.10 (i) | Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. | Ensure your team is properly trained to use Confluence and the approval process. Maintain training records. |  |
| 11.10 (j) | The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. | Implement awareness and accountability policies to ensure that login information is not shared with other individuals and that signatures are not performed by another person. |  |
| 11.10 (k)(1) | Use of appropriate controls over systems documentation including:  
1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.  
2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | System documentation may be managed within Confluence, using the approval mechanism provided by Conala Document Management. If system documentation is managed in Confluence, then use Confluence’s “provide access” segregation mechanisms to protect it. Manage system documentation securely. If managed in Confluence, this information should also be exported so that it can be used when the system is down (ie, for recovery). This information should be secured to avoid a security breach. |  |
Compliant Electronic Document Management Systems ensure that signed electronic documents contain information associated with the signing, clearly indicating all of the following:

1. The printed name of the signer.
2. The date and time when the signature was executed.
3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Comala Document Management provides the 'Page Activity' report. This report provides the following data for each approval (electronic signature):

1. The full name of the user
2. Date and time of approval
3. The name of approval, which constitutes the meaning of the signature.

The Page Activity report can be embedded in the Confluence page and included in exports.

11.50 (b)  The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Include the Page Activity report in official exports.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

The linkage between approvals and the Confluence pages is part of the internal database tables and cannot be falsified through manipulation of the page.

Subpart C - Electronic Signatures

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement (the original wording is given in italics)</th>
<th>How to Achieve Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.50 (a)</td>
<td>Comalatech Apps</td>
<td>Confluence Processes and Activities</td>
</tr>
<tr>
<td>11.100 (a)</td>
<td>Each electronic signature shall be unique to one individual, and shall not be reused by, or reassigned to, anyone else.</td>
<td>Put policies in place to ensure unique ID's are not reused or reassign ed. This can be achieved through a User Management /Director y Solution.</td>
</tr>
<tr>
<td>Section</td>
<td>Text</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11.100 (b)</td>
<td>Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.</td>
<td>The identity of individuals should be verified before they are granted access. This is typically part of staff on-boarding.</td>
</tr>
<tr>
<td>11.100 (c)</td>
<td>Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.</td>
<td>This requires you to submit to the FDA a document in regards to your use of electronic signatures.</td>
</tr>
<tr>
<td>11.200 (a)(1)</td>
<td>Electronic signatures shall employ at least two distinct identification components, such as an identification code and password.</td>
<td>In Comala Document Management, an individual electronically signs an approval by providing their Confluence access credentials: username and password. These credentials are validated through Confluence's authentication interface.</td>
</tr>
<tr>
<td>11.200 (a)(1) (i)</td>
<td>When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.</td>
<td>Comala Document Management requires that full credentials are provided for each signature. These are composed of two elements: username and password.</td>
</tr>
<tr>
<td>11.200 (a)(1) (ii)</td>
<td>When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.</td>
<td>Comala Document Management requires that full credentials are provided for each signature. These are composed of two elements: username and password.</td>
</tr>
<tr>
<td>11.200 (a)(2)</td>
<td>(Electronic signatures) shall be used only by their genuine owners</td>
<td>Implement awareness and accountability policies to ensure that login information is not shared with other individuals and that signatures are not performed by another person. Implement security measures on the infrastructure level to protect and identify breaches.</td>
</tr>
<tr>
<td>11.200 (a)(3)</td>
<td>(Electronic signatures) shall be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</td>
<td>Confluence provides certain protections to password information (i.e., encryption). More information is provided here. The infrastructure including any user directory and user access mechanisms need to be setup in a way that protects from the possibility of: These protections alone are not sufficient to meet this criteria, but should be seen as part of the solution.</td>
</tr>
</tbody>
</table>
1. re-setting of password information by a single administrator (which will then enable them to posture as another user).

2. theft of password information.

3. breach of access and fraudulent signature.
| 11.300 (a) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. |

| In Confluence, username is a unique identifier. |

| Any active directory and user sign-on mechanisms should be set in a way that ensures uniqueness across the board. |

| 11.300 (b) | Ensuring that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging). |

| Confluence provides the means to make users 'inactive'. That way users may be blocked from accessing the system without losing their historical data. |

| Put policies in place to ensure that your user list and access rights are current. For example: |

1. off-boarding of staff needs to include disconnection of their respective user accounts. |

2. access rights are periodically reviewed. |
| 11.300 (c) | Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | If you are using tokens or other devices to help gain system access, take measures to manage theft, loss etc of those devices. |
| 11.300 (d) | Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | Install Confluence on a secure infrastructure, and use SSH communication. Implement security monitoring and protection. |
| 11.300 (e) | Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. | Relates to a scenario in which you are using tokens or other devices to help gain system access. |

2.1 Find out more...

For more information contact us at support@comalatech.com or directly to our support system at https://comalatech.jira.com/servicedesk/

(c) 2019 Comala Technology Solutions, Inc.