Spotfire™

Spotfire white paper

Spotfire® product family

Compliance with 21 CFR Part 11, GxP, and related software validation issues

Executive summary

The Code of Federal Regulations Title 21 Part 11 (commonly referred to as 21 CFR Part 11) establishes requirements for electronic records and electronic signatures (ERES) applicable to biotechnology and drug development companies, medical device manufacturers, contract research organizations, and other industries regulated by the US Food and Drug Administration (FDA). The regulation requires the implementation of validations, audit trails, and other controls for systems involved in the processing of electronic data and records required by the FDA.

As a long-standing provider of software to customers in regulated industries, Spotfire® has formalized procedural as well as functional requirements to ensure that its products can operate within the framework provided by 21 CFR Part 11 and the FDA's Guidance for Industry documents. Spotfire product development and support is governed by an integrated business management system (BMS) conforming to widely acknowledged standards for quality management and information security management.

Multiple tools dedicated to system validation are included in the Spotfire product portfolio, and specific capabilities relevant to regulatory compliance have been developed in cooperation with leading pharmaceutical and biotechnology companies, as well as strategic partners, taking FDA guidelines and common industry practices into account.

Spotfire has been successfully audited by a large number of companies whose concerns include 21 CFR Part 11 and GxP compliance and related software validation issues. This white paper provides an overview of how Spotfire products address such issues as an essential part of many customers' business needs. With a focus on the "predicate rule" requirements (controls mandated by the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act) outlined in 21 CFR Part 11.10 and 11.30, as driven by Good Practices Regulations of Title 21 (including Part 58 / GLP, Part 312 / GCP, and Part 210 / CGMP), the paper demonstrates that applications based on Spotfire products can readily ensure that electronic records are trustworthy and reliable.

Spotfire products and components

As a leading platform for visual analytics and data science, Spotfire offers a wide range of capabilities that enable customers to turn data into actionable insights. Spotfire products and associated functional components can be configured, integrated, and deployed according to the specific needs of individual customers, on their own, or as part of a larger system. A brief overview of components is provided below.

Core components

The core part of the Spotfire platform provides an extensive set of capabilities to support generic analytics use cases, such as the ability to:

- Access and manage data from different sources
- Visualize and interactively explore data (ad hoc/exploratory analysis)
- Create and use dashboards, analytic applications, and similar solutions (guided analysis)
- Capture and share insights
- Automate tasks

Customers can create analytic applications targeted at more specific use cases where compliance with 21 CFR Part 11 may be relevant. Depending on the scenario, such use cases can involve filtering, aggregating, drilling down, performing calculations, applying statistical methods, and other interactions.

Functional components include the core Spotfire application (data engine and visualization framework), multiple client interfaces (desktop, web, mobile), a Spotfire Server, Spotfire Data Connectors, and Spotfire Automation Services. The Spotfire Qualification tool can also be used to support system validation.

Data science components

The data science part of the Spotfire platform includes capabilities for authoring and deploying data science workflows and scripts, typically based on Spotfire Statistica®. Examples of use cases where compliance with 21 CFR Part 11 may be relevant include:

- Test the characteristics of new products
- Optimize product formulations
- Inspect raw materials to be used in the manufacturing of products
- Judge the efficacy of multiple product configurations
- Predict product reliability
- Determine the most important process parameters within a multivariate manufacturing application
- Certify that particular lots of product conform to specifications
- Produce annual product quality review reports

Such use cases can involve creating and using templates (data cleaning, data mashup, analytic workflow), validating data, writing validated data back into a database, emailing tabular and graphical results, generating PDF reports, and using dashboards.

Functional components include an Enterprise Manager application for managing metadata store objects and a Data Entry Server. The Enterprise Manager integrates with Active Directory and supports role-based security, versioning, electronic signatures, and audit logs. When data is manually entered in a web form, signatures, comments, and approvals will be captured in accordance with 21 CFR Part 11 requirements.

Streaming components

The streaming part of the Spotfire platform (using Spotfire® Streaming) supports use cases that involve streaming of live data into Spotfire, such as real-time assessment, anomaly detection, and dynamic learning.

Quality of products and services

The Spotfire software development life cycle (SDLC) constitutes a core part of Spotfire's integrated business management system, the quality part of which has been certified according to ISO 9001. The SDLC contains documented processes and procedures for product requirements management, design, implementation, validation, release, support, and retirement.

Program planning

In the program planning phase, customer and other stakeholder requests and supporting information, such as use cases, are collected and captured as product requirements by Spotfire Product Management. The requirements are reviewed, refined, and prioritized based on estimated value and cost.

In parallel with these activities, the Spotfire Engineering team works out a plan for the next product release. The plan specifies targeted requirements and planned milestones, taking into account available resources, technical and architectural aspects, and risks. Engineering and Product Management are jointly responsible for change management at the program level.

Design and implementation

The design and implementation phase includes activities performed by multiple functions, including team management, design and development, documentation, and testing.

Team leaders are responsible for continuous detailed planning, change management at the team level, and retrospectives intended to identify issues and opportunities for improvement. Design and development activities include creation and review of design documents, coding, code reviews, and defect fixing. Test cases are developed in parallel with the design so that testing can be initiated as early as possible. Unit tests are automatically executed every time the source code is modified, and developers are immediately notified of any failed tests.

In some cases, design and implementation can include an alpha and/or beta phase, one purpose of which is to collect feedback that can be used to address issues and opportunities for further enhancements.

Validation

The validation phase begins when all planned features have been implemented, and involves additional testing of the integrated software. Integration and testing occur continuously throughout the design and implementation phases so that the smallest possible number of defects will be detected during validation. Testing involves a range of manual and automated techniques with a focus on various quality aspects. A test plan describes the planned test scope for different areas, and the resources needed to conduct necessary feature and system-level testing. Regression testing ensures that functionality continues to work as expected. Secure development practices are also in place to ensure that potential security issues, such as vulnerabilities in third-party software, are identified and addressed promptly.

Toward the end of a release cycle, the source code is locked down, and any further changes require explicit approval and a stringent code review. Test results and other validation artifacts are reviewed to determine that all applicable requirements have been fulfilled and that the software meets the overall criteria for release.

Release

Product release to the market is governed by a detailed general availability (GA) release process, which covers product components, documentation, licensing, approval of third-party software, and sign-off by a cross-functional group of stakeholders. Once products have been approved for general availability, the software and associated documentation are made available through applicable channels (on-premises and/or hosted), and customers are notified of the release.

Support and maintenance

After release, Spotfire's Global Support team provides support and contributes to defect prioritization in maintenance releases. A Support portal provides easy access to useful resources, such as product documentation, Spotfire Community content, Support knowledge base, and hotfixes. Customer satisfaction surveys and other mechanisms are in place to promote the quality of support services.

Security of information

Spotfire relies on a comprehensive set of controls to protect the confidentiality, integrity, and availability of information relevant to its customers and other important stakeholders. A variety of controls are in place to restrict access to facilities, networks, hardware, software, and other assets used in the development and support of Spotfire products. Information security is also an integral part of the Spotfire SDLC, and a risk management program is used to ensure that information security risks are handled appropriately. The information security part of Spotfire's integrated business management system has been certified according to ISO 27001.

Continuity of business

The Spotfire business unit maintains a business continuity plan (BCP) to be followed in case of a disruptive event. The BCP outlines steps appropriate to the nature of the event to ensure continuity of business operations. Spotfire has staff in multiple offices on several continents. The Engineering team is distributed, with the largest groups in Gothenburg, Sweden, and Pune, India. Spotfire IT infrastructure is shared with other business units within Cloud Software Group and is mainly located in the United States.

Qualified staff

Qualified personnel are critical to the development of software products for use in regulated environments. Spotfire staff includes many individuals with highly developed software engineering skills, and some with significant subject-matter expertise in bioinformatics and applied life sciences. Several members of the Engineering team hold doctoral degrees. In addition to regular training courses, staff competence is further developed using a broad spectrum of activities, such as mentoring, participation in competence networks, interaction with customers and partners, and research. Specialized courses developed in-house for customers are also made available to Spotfire staff.

Compliance with 21 CFR Part 11

This section describes how systems that include Spotfire software can comply with individual regulations in 21 CFR Part 11. Depending on what products and components are used, compliance can be achieved using out-of-the-box functionality and/or product platform capabilities specifically configured in accordance with individual customer needs.

11.10 Controls for closed systems

11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
FDA validation guidelines state that end user needs and intended uses of the system must be established, and that evidence that the system meets those needs must be traceable to the system design and specification. Within Spotfire itself, the tasks needed to plan, develop, release, and maintain products are consistently performed in accordance with a well-defined software development life cycle by staff with the knowledge and skills to perform their job functions effectively.

The core Spotfire product supports the design, development, and validation of dashboards, analytic applications, and similar solutions, as well as integration with computing systems and host environments through a range of product features and associated capabilities that enable the system as a whole to be compliant with 21 CFR Part 11.

In Statistica, a read-only audit trail tracks login/logout, creation, modification, deletion, and approval of objects along with computer-generated date and time stamps. Web forms can be configured to prevent invalid data from being saved with the "complete" status. To validate entered data, the user can select from a pull data list or only enter a number (e.g., > .081 AND < .089). Complex formulas can be written to use multiple fields from the web form. The web forms for manual data entry can use double-blind data entry for verification of accuracy. Two individuals enter the same data (record). They mark the records as "complete". The system captures electronic signatures that the records are complete and compares the two records. If the records don't match, they are both rejected, and email notifications are sent to correct the issue. If the two records are identical, the system marks this set as an approved record.

11.10(b) 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.
Spotfire understands this to mean that the system must be capable of rendering any records required by an auditor in a format that can be read, understood, and copied by computers (e.g., by exporting the records to file) as well as humans (e.g., by printing the records, possibly after first exporting them to a file), without in any way affecting the accuracy or completeness of the records.

In the context of the core Spotfire product, several types of objects could potentially be used to represent a record in a specific application. Examples include:

- A portion of a data table (e.g., a row) or TERR object
- A portion of a visualization (e.g., a group of markers in a scatter plot)
- A portion of a text area with static or dynamic (e.g., script-generated) contents

The core Spotfire product is capable of reading and writing data in a variety of industry-standard formats. In addition, other products are capable of reading and writing data stored in Spotfire-defined formats. Thus, data table records can be made available in machine-readable form independently of the use of Spotfire products. Products from other vendors can also be configured to print human-readable reports from the same data. Similarly, records represented by graphical entities, which are derived from data tables and metadata, can be printed and exported to a range of industry-standard file formats. Spotfire data functions, which can be used to enrich the analysis of both tabular and graphical records, are expressed in a language that is both human and machine-readable.

Building on the capabilities outlined above, the highly configurable nature of the core Spotfire product provides multiple ways in which applications can readily generate copies of records that are both human and machine-readable, thereby enabling other business needs (such as the appropriate level of visual interactivity) of individual customers and partners to be balanced against system complexity and other important considerations. To verify accuracy and completeness, the Spotfire Qualification Tool can be used to programmatically compare application output to a predefined, manually inspected "gold standard."

In Statistica, audit logs can be retrieved, filtered, and saved as PDFs for easy sharing. Analytic results, metadata, or raw data can be viewed within the system in spreadsheets or reports. This information can also be exported to Excel, Word, or sent by email. Manually entered data can be reviewed within a web browser or retrieved for analysis.

11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
Spotfire understands this to mean that any records processed by the system must be protected against change (e.g., through intentional or accidental deletion or modification, technical issues, external or environmental threats) and readily retrievable throughout whatever period of time is deemed necessary.

As outlined under item (b), the core Spotfire product is capable of generating accurate and complete copies of records in human and machine-readable form, in a location specified by the application (as determined by its design and host environment) and/or the system operator. Records exported to file can be retrieved through execution of the software or other commonly available tools. The Spotfire product will not automatically delete or modify such records. Printed records can be retrieved by a mechanism to be defined by individual customers. Other aspects of information security (which includes integrity and availability of records) are addressed through a wide range of controls implemented in accordance with ISO 27001 requirements.

Building on the capabilities outlined above, it is the responsibility of individual customers to implement and configure any local controls (for example, access restrictions, backup, malware protection, protection against physical hazards, and others) needed to ensure that records generated by the system remain accurate and readily retrievable throughout the required time period.

In Statistica, all records and their metadata, including older versions, can be readily retrieved, viewed, and used in reports.

11.10(d) Limiting system access to authorized individuals.
Spotfire understands this to mean that only those individuals who have explicitly been granted permission should be able to access system components, including Spotfire products and applications, and any records processed or generated by the system.

While item (c) addresses the integrity and availability aspects of information security, item (d) addresses the confidentiality aspect. The core Spotfire product uses technical controls needed to support this aspect in accordance with ISO 27001 requirements. This includes features that enable customers to implement appropriate user access management (user names, user groups, roles) and system and application access control mechanisms (access restrictions, secure log-on) with the appropriate level of granularity. A variety of options are available to support integration with security mechanisms in the host environment.

Building on the capabilities outlined above, individual customers are enabled to configure a very robust system in compliance with item (d) and local information security policies.

Spotfire Statistica integrates with Active Directory user accounts. When the system is configured, we recommend setting up synchronization with the domain. This allows it to add and delete users based on domain groups. As long as the domain groups are kept updated, IT does not need to log in to the Statistica system to add or delete users and existing security processes can be used.

Spotfire Statistica has multiple levels of security. The user has to be granted access to use a specific application. Within the application, they need to be granted read or edit permissions to use specific configuration objects.

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.

Spotfire understands this to mean that the system must automatically document the complete sequence of actions that alter electronic records processed by the system, in such a way that the local time and nature of each event can be readily viewed and copied by auditors and other authorized persons, and that the documentation must be protected against change and readily retrievable throughout the retention period of the underlying records.

The core Spotfire product supports the automated generation of audit trails with its ability to produce complete time-stamped log files. The Spotfire expression language contains functions that enable time-stamping of records and operator entries throughout the application. These and other technical controls for logging and monitoring have been implemented in accordance with ISO 27001 requirements. Confidentiality and protection against change can be achieved through proper integration with the host environment and with the mechanisms discussed under items (c) and (d).

Building on the capabilities outlined above, customers and partners are readily enabled to meet the FDA requirements for audit trails. It is the responsibility of individual customers to implement and configure any local controls (e.g., clock synchronization) needed to ensure the accuracy and completeness of audit trails.

In Statistica, the audit log options are configured shortly after installation. Actions such as login/logout, create, modify, or delete can be logged with a change reason, date and time stamp, and user name. There is a configuration option to turn on audit logging and prohibit any changes to the logging. In other words, once this option is turned on, it cannot be turned off.

Note: The delete action mentioned above is the deletion of a template or configuration object by an administrator. It is not possible for a user to delete the audit log within the application.

11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
Spotfire understands this to mean that the system must ensure that it is not possible for a system operator, or the system itself, to cause deviations from acceptable workflows.

The core Spotfire product is designed to support a continuum of analytic environments and use cases, ranging from unrestricted exploratory analysis, via guided analytic applications that offer a certain degree of freedom, to applications that completely enforce a strict workflow. Thus, a combination of application design and product features can be used to restrict the ability of system operators to perform certain functions under certain conditions and to enforce a certain permitted sequence of steps and events. An even higher degree of customization can be achieved through scripting and/or coding.

In Statistica, users create analytic workflow templates to sequence data cleaning and analytic steps. They create validation rules and sequences for web forms used for manual data entry, such as:

- If "field 1 on form 1" > .066 then "field 2 on form 3" must be < .1, otherwise error and don't let form 3 be saved.

The sequence of create, edit, review, and approve is handled within the Enterprise Manager.

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.
Spotfire understands this to mean that the system must prevent persons who have not explicitly been granted permission to interact with the system in a certain way (e.g., to access the system and/or records processed by the system, alter and/or electronically sign a record, and more) from doing so.

As discussed under other items, and item (d) in particular, the core Spotfire product has the technical controls needed to support the confidentiality aspects of information security in accordance with ISO 27001 requirements. Compliance with the FDA requirements for authority checks can be achieved by using product features such as the Administration Manager and library administration tools, which determine access to functionality, data connectors, data sources, library folders, and other entities, for individual users and groups of users, and through integration with related mechanisms implemented in the host environment.

Spotfire Statistica integrates with Active Directory login accounts, which use a combination of a username and password to authorize an electronic signature. The system uses role-based security and verifies if an individual has the right to start Statistica software, manually enter data, review and approve manually entered data, create templates, use templates, modify a specific template, log in to a website, and other operations.

11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
Spotfire understands this to mean that the system must ensure that any input (including data and operational instructions) comes from a legitimate source (e.g., entered by a system operator or imported from a particular database) and is otherwise valid (e.g., has the correct data type and format).

Like in the discussion about operational system checks under item (f), the core components of the Spotfire platform support input validation through a combination of application design and product features that can be used to prevent system operators from entering invalid input or importing data from an illegitimate data source. Compliance with the FDA requirements for device checks can be achieved using those features and through integration with related mechanisms implemented in the host environment.

Spotfire Statistica uses role-based security to grant access to applications or objects within applications. Users are typically granted a role by belonging to a specific Active Directory group. The system can be configured to require electronic signatures (login and password that verify identity) when manually entered data is saved, marked "complete", and approved. The system also collects electronic signatures when objects are approved.

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.
While it is primarily the responsibility of individual customers to ensure compliance with this item, also see item (a) and the section about qualified staff within Spotfire itself.

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.
It is the responsibility of individual customers to establish and enforce the policies required by this item.

The Spotfire product family includes functionality that enables policies to be exposed or referenced within the system.

11.10(k) Use of appropriate controls over systems documentation include:
(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.
Spotfire understands this to mean that any documentation necessary for the proper operation and maintenance of the system (for example, SOPs and validation documents) must be managed in a controlled manner by applying suitable and adequate document control mechanisms (including archival of obsolete versions) and that the documentation must be readily available to, and used as intended by, relevant stakeholders.

All releases of Spotfire products include documentation developed in accordance with the Spotfire SDLC, as well as the procedures that govern the control of documents, both of which have been certified according to ISO 9001.

Similar to the source code, the documentation is managed in a revision control system and covers installation, administration, operation, and application configuration, as applicable. All documents are uniquely identifiable and connected to a specific release of the software. The documentation is provided to clients in an electronic format, through a dedicated documentation website. Release notes are available from the Support portal.

It is the responsibility of individual customers to handle Spotfire product documentation at the client site, and to create and manage any additional documents needed for proper operation and maintenance of specific applications deployed in the host environment.

11.30 Controls for open systems

Briefly, section 11.30 states that controls for open systems (in which contents and user access are not controlled by the same party) shall include those identified in section 11.10, as appropriate, and any additional measures regarded as necessary under the circumstances. Compliance can be achieved by using Spotfire product features and associated capabilities discussed for closed systems, and item 11.10(d) in particular, and through integration with mechanisms implemented in the host environment. It is the responsibility of individual customers to ensure that appropriate safeguards are implemented at the client site.

11.50 Signature manifestations

11.50(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
When integrated login with Active Directory is used, the electronic signature is the domain\login name and password that was used to sign into the computer. Spotfire Statistica automatically captures the date and time stamp with the signature. The system can be configured to record the meaning of the signature.

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).
In Statistica, this information is displayed in a read-only audit trail. A PDF report can be generated with this information.

11.70 Signature/record linking

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.
In Statistica, an electronic signature is linked to a specific version of an object that contains information about the purpose of the signature and the record(s) it is intended to authorize. This linked information is stored in the metadata store. From within the system, it is impossible to remove, modify, or transfer an existing electronic signature.

11.100 General requirements

11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
The recommended approach for ensuring compliance with item 11.100(a) is integrating the system with Active Directory logins so the customer's established security processes can be used.

11.100(b) 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.

11.100(c) 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.
It is the responsibility of individual customers to ensure compliance with items 11.100(b) and (c).

11.200 Electronic signature components and controls

11.200(a) Electronic signatures that are not based upon biometrics shall:
(1) Employ at least two distinct identification components such as an identification code and password.
(2) Be used only by their genuine owners; and
(3) 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.
The recommended approach for ensuring compliance with item 11.200(a) is integrating the system with Active Directory logins so the customer's established security processes can be used. Spotfire Statistica always collects the domain\login account and password for electronic signatures.

11.200(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
Not applicable: Spotfire software does not use biometric authentication techniques.

11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. The recommended approach for ensuring compliance with items 11.300(a) through (e) is integrating the system with Active Directory logins so the customer's established security processes can be used.

Conclusion

Spotfire provides a solid foundation for regulatory compliance through its comprehensive software development life cycle, qualified staff, and other necessary controls established within an integrated business management system conforming to ISO 9001 and ISO 27001.

Capabilities that enable systems to comply with 21 CFR Part 11 requirements and ensure that electronic records are trustworthy and reliable are managed in accordance with well-defined processes and procedures throughout the entire life cycle. Depending on the specific needs and intended use cases of individual customers and partners, compliance with FDA requirements can be achieved by selecting, configuring, and deploying the most appropriate products and components, and through integration with the host environment at the client site. This approach makes it straightforward to balance simplicity of compliance with other important business needs to be fulfilled by the system. It also provides clarity with respect to system operation and puts system expertise closer to the customer, where it belongs.

The Spotfire product family has been designed to provide both generic and industry-specific visual analytics and data science capabilities needed to support critical business decisions and to allow individual customers to expose required capabilities in a user experience that is appropriate to their needs. As a case in point, Spotfire has been serving the clinical development industry for more than 25 years and takes its role in this regulated environment very seriously.

References

- FDA Title 21 CFR Part 11: Electronic Records; Electronic Signatures; Final Rule (1997).
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff (2002).

Spotfire™

Cloud Software Group
Headquarters
851 W Cypress Creek Rd.
Fort Lauderdale, FL 33309
www.spotfire.com