TIBCO Spotfire Product Family

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

The Code of Federal Regulations Title 21 Part 11 (commonly referred to as 21 CFR Part 11) is a requirement of the FDA's drug application process. The regulation requires drug sponsors to implement validations, audit trails, and other controls applicable to software systems involved in processing of electronic records required by the FDA. As a long-standing provider of software to the biopharmaceutical community and associated industries, TIBCO has taken steps to ensure that its products are able to operate within the framework provided by 21 CFR Part 11 and the FDA's Guidance for Industry documents.

The TIBCO Spotfire product family is widely used for data management, analysis, and various kinds of reporting. Many product capabilities 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 products adhere to globally acknowledged standards regarding software development, quality management (including ISO 9001), and information security management (including ISO 27001). Well defined processes have been established to ensure that applications based on Spotfire products can meet necessary requirements, including 21 CFR Part 11. Tools dedicated to aid customers in validating application installations have been included in the TIBCO Spotfire product family since 2011.

Spotfire analytics 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 whitepaper provides an overview of how Spotfire products address such issues as an essential part of many customers' business needs. With focus on the "predicate rule" requirements (controls mandated by the 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.

System Validation

System validation is a challenge for any company operating in a regulated environment. Regulation 21 CFR Part 11.10(a) requires validation of computer systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. More specifically, 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. Further, Part 11.10(i) requires persons who develop and maintain the system to have adequate competence in terms of education, training, and experience.

Validation of Spotfire applications relies on compliance with effective controls reflecting these requirements. Within Spotfire software, the tasks needed to plan, develop, release, and maintain products are consistently performed in accordance with a well-defined software development lifecycle (SDLC) by staff with the knowledge and skills to perform their job functions effectively. The SDLC constitutes a core part of the Spotfire quality management system, which is certified according to ISO 9001. Additional controls ensure the ongoing security and integrity of systems developed by TIBCO. The sections below summarize these controls, and explain how they enable software systems that include Spotfire products to comply with 21 CFR Part 11.10(a) and (i).

Software Development Life Cycle

Product and Release Planning

The Spotfire software development lifecycle begins with a product and release planning phase, during which customer and other stakeholder requests and supporting information, such as use cases, are collected and captured as product requirements. The requirements are reviewed, refined, and prioritized based on estimated value and cost. Clearly specified acceptance criteria must exist before a requirement can be approved.

In parallel with these activities, the TIBCO 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, risks, etc.

Design and Implementation

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

Dedicated team leaders are responsible for continuous detailed planning, regular retrospectives intended to identify issues and opportunities for improvement, and change management at the team level. Design and development activities include creation and approval of design documents, coding (including unit testing and product integration), code reviews, and defect fixing. As described below, test cases are developed in parallel with the design, so that testing can be initiated as early as possible. Furthermore, a configuration management function ensures that a product build is created, and a comprehensive suite of test cases automatically executed every time the source code is modified. Development teams 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 to further enhance the product.

Validation

In the Spotfire software development lifecycle (SDLC), the validation phase begins when all planned features have been implemented, and involves additional testing of the integrated software. However, as indicated above, integration and testing occur throughout the design and implementation phase, the intention being that the smallest possible number of defects will be detected during validation. For that purpose, testing

involves a wide variety of manual and automated techniques with focus on various quality aspects. A system test plan describes the planned test scope for different areas, and the resources (including test environments) needed to perform the tests. Procedures for management of test cases enable teams to perform necessary feature testing as well as system level testing. Regression testing is performed to ensure that functionality continues to work as expected. Towards the end of a release cycle, the source code is locked down, and any further defects are not allowed to be fixed without explicit approval and a stringent code review.

The acceptance criteria defined earlier are used to ensure that the software meets specified requirements and fulfills intended uses. As an additional safeguard, the Spotfire Qualification Tool is used internally to compare product output against a predefined, manually inspected "gold standard."

Release

When the validation phase has been successfully completed, the release coordinator within the Spotfire group reviews recorded product changes and collects evidence that all required artifacts have been finalized and approved in accordance with SDLC requirements, and that the software meets the criteria for release.

Product release to the market is governed by a detailed general availability (GA) release process, which covers product components, documentation, licensing, and packaging approval of third party software, and sign-off by a cross functional group of stakeholders. Any externally supplied products and processes are reviewed and qualified, where necessary, prior to acceptance. Once the product has been approved for general availability, the software and associated documentation is made available on TIBCO's digital fulfillment site and customers are notified of the release. The source code is archived and securely placed in escrow.

Maintenance, Support, and Retirement

After release, TIBCO'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, TIBCO Community contents, a support knowledgebase, and product hotfixes. Customer satisfaction surveys and other mechanisms are in place to promote quality and consistency in support services.

Qualified Personnel

Qualified personnel are critical to development of software products for use in regulated environments. TIBCO Spotfire staff includes many individuals with highly developed software engineering skills, and some with significant subject-matter expertise in bioinformatics and applied life sciences. A number of 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.

Supporting Controls

Information Security

TIBCO has implemented a comprehensive set of controls to protect the confidentiality, integrity, and availability of information relevant to its customers and other important stakeholders. For example, an HR security policy governs information security aspects of people management prior to, during, and after employment. A variety of controls are in place to restrict access to facilities, networks, hardware, software, and other assets used in development of Spotfire products. Information security is also an integral part of the Spotfire SDLC, and a risk management process is used to ensure that information security risks are handled in an appropriate manner. The complete set of controls constitutes a core part of the Spotfire information security management system, which is certified according to ISO 27001.

Business Continuity and Disaster Recovery

TIBCO maintains business continuity and disaster recovery plans to be followed in case of a disruptive event. These plans outline steps appropriate to the nature of the event to ensure continuity and recovery of business operations.

TIBCO has multiple offices on several continents. The TIBCO Spotfire group has a distributed engineering team with offices in Seattle, WA; Gothenburg, Sweden; Paris, France; and Pune, India. TIBCO IT infrastructure is located in Palo Alto, CA; Seattle, WA; and Gothenburg, Sweden.

Compliance Enabling Functionality

In addition to the controls described in the previous section, the Spotfire product family supports integration with 21 CFR Part 11 compliant computing systems and host environments through a range of product features and associated capabilities that enable the system as a whole to be compliant. A description follows of how each control (excluding those covered in the previous section) in sections 11.10 (for closed systems) and 11.30 (for open systems) can be addressed with Spotfire functionality. The description includes a brief summary of TIBCO's interpretation of the meaning of the control.

Controls Aand TIBCO Spotfire Capabilities

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.

TIBCO understands this item to mean that the system (as defined in the overview) must be capable of rendering any records required by an auditor in a format that can be read, understood, and copied by computers (for example, by exporting the records to file) as well as humans (for example, 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 Spotfire products, several types of objects could potentially be used to represent a record in a specific application. Examples include:

- A portion of a data table (for example, a row) or TIBCO Enterprise Runtime for R (TERR) object
- A portion of a visualization (for example, a group of markers in a scatter plot, or a line in a line chart)
- A portion of a text area with static or dynamic (for example, script generated) contents

Spotfire products are 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 TIBCO and 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 Spotfire products 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."

11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

TIBCO understands this item to mean that any records processed by the system must be protected against change (for example, through intentional or accidental deletion or modification, technical issues, external or environmental threats, and more) and readily retrievable throughout whatever period of time is deemed necessary.

As outlined under item (b), Spotfire products are 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. Spotfire products 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.

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.

11.10(d) Limiting system access to authorized individuals.

TIBCO understands this item to mean that only those individuals who have explicitly been granted permission should be able to access the system and its constituent components, including Spotfire products and applications, and any records processed or generated by the system.

While item (c) addresses the integrity (I) and availability (A) aspects of the "CIA triad" that is central to information security, item (d) addresses the confidentiality (C) aspect. The Spotfire product family uses technical controls needed to support this aspect in accordance with ISO 27001. 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 the security mechanisms available in the host environment, taking into account the needs of individual customers.

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.

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.

TIBCO understands this item 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.

Spotfire products support 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. 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 (for example, clock synchronization) needed to ensure the accuracy and completeness of audit trails.

11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

TIBCO understands this item 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.

A core part of the Spotfire design philosophy, which is reflected throughout the product architecture, is 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. This is achieved through a combination of application design and product features that 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.

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.

TIBCO understands this item to mean that the system must prevent persons who have not explicitly been granted permission to interact with the system in a certain way (for example, 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 Spotfire product family has the technical controls needed to support the confidentiality aspects of information security in accordance with ISO 27001. Compliance with the FDA requirements for authority checks can be achieved by using Spotfire 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.

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.

TIBCO understands this item to mean that the system must ensure that any input (including data and operational instructions) comes from a legitimate source (for example, entered by a system operator or imported from a particular database) and is otherwise valid (for example, has the correct data type and format).

Like in the discussion about operational system checks under item (f), the Spotfire product family supports 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.

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 including:

- Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
- Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

TIBCO understands this item 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 corporate procedure governing control of documents, both of which are 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. 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 TIBCO's public documentation web site.

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.

Conclusion

TIBCO Spotfire software provides a solid foundation for regulatory compliance through its development lifecycle, its qualified personnel, and supporting controls established within an integrated management system that is certified according 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 throughout the entire lifecycle, from product and release planning to maintenance and support. Through a fundamental benefit of its design philosophy, the core of the Spotfire product family makes it possible to satisfy most requirements in more than one way. Depending on the specific needs and intended uses of individual customers and partners, compliance with FDA requirements can be achieved through configuration of the most appropriate capabilities, 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 individual customer, where it belongs.

The Spotfire product family has been designed to provide users with capabilities that support general capabilities as well as industry specific needs and the user experience and analytic power needed to support critical business decisions. As a case in point, TIBCO Spotfire analytics 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).

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

21Oct2019