ASPECTS OF IMPLEMENT A RISK BASED COMPUTER VALIDATION PROGRAM IN information technology of Business continuity management

Lebedynets V. O., Chornyi D. S., Podlesnaya A. V.**

The National University of Pharmacy, Kharkiv, Ukraine

*** LLC "Business Center Pharmacy", Vyshgorod, Ukraine**

In recent years the industry has been moving towards the implementation of a risk based computer validation approach. This creates the challenge about how to implement a risk-based computer validation program.

When concluding contracts between manufacturers of drugs of other countries and importers (distributors) of drugs in the territory of Ukraine, there is often a requirement to provide distributors business continuity management.

This Guide GAMP 5 “Risk-Based Approach to Compliant GxP Computerized Systems” describes in Appendix O10 the key requirements, process, guidance required to restore business processes following a disruption while continuing to provide product to the customer.

Business Continuity planning (BCP) is about the ability to respond to any interruption that impacts the ability to deliver products and services. The BCP will identify the triggers for invocation of the plan, people to be involved and required communication, as well as the interim processes to manage the disruption.

BCP need to focus only on how to respond; what tasks should be performed in case of violation. If planning is right, then what products and services are critical to business and what assets (tools, people, technology, business processes, and supply chains) are critical to delivering these products and services. It needs to be able to plan for the recovery, replacement, or continuity of these assets, regardless of the fact that they were broken.

When forming the process of continuity, one of the key issues is the issue of information security, in particular the resources involved in ensuring the continuity of business (data, hardware and software complexes, relevant personnel). It will be necessary to identify critical business processes, which can be recovered through technical means, impact on business, risk analysis and the direct formation of the process of ensuring the continuity of business.

General Approach:

- Regulated companies should define a process for the production of BCPs including the use of common formats. It is likely that a BCP will cover many systems. A risk-based approach to the content and detail should be taken so that each system is adequately covered;

- BCPs and their rehearsals should be subject to periodic internal audits.
- Consideration should be given to maintaining BCP procedures off-site and maintaining the information on paperbased systems.
- The communication process is an important aspect of BCP, key contacts (e.g., process owner, system owner, suppliers and quality unit) should be listed with contact details.
- The BCP should include a clear process for prioritizing system restore as the disruption may involve failure or unavailability of multiple systems which may be within or outside the regulated company.
- Where manual processes are invoked to allow the business to continue to operate, it is important to consider how any associated electronic records or data will be synchronized once the electronic systems have been restored.
- The BCP should consider the need for defining both short-term and long-term business continuity options and when they might be used.

- Business Continuity Plans can be rehearsed or tested in several ways, such as through reviews, brainstorming, walkthroughs, testing of sections of the plan, re-installation of servers, switching to hot sites, and full testing.

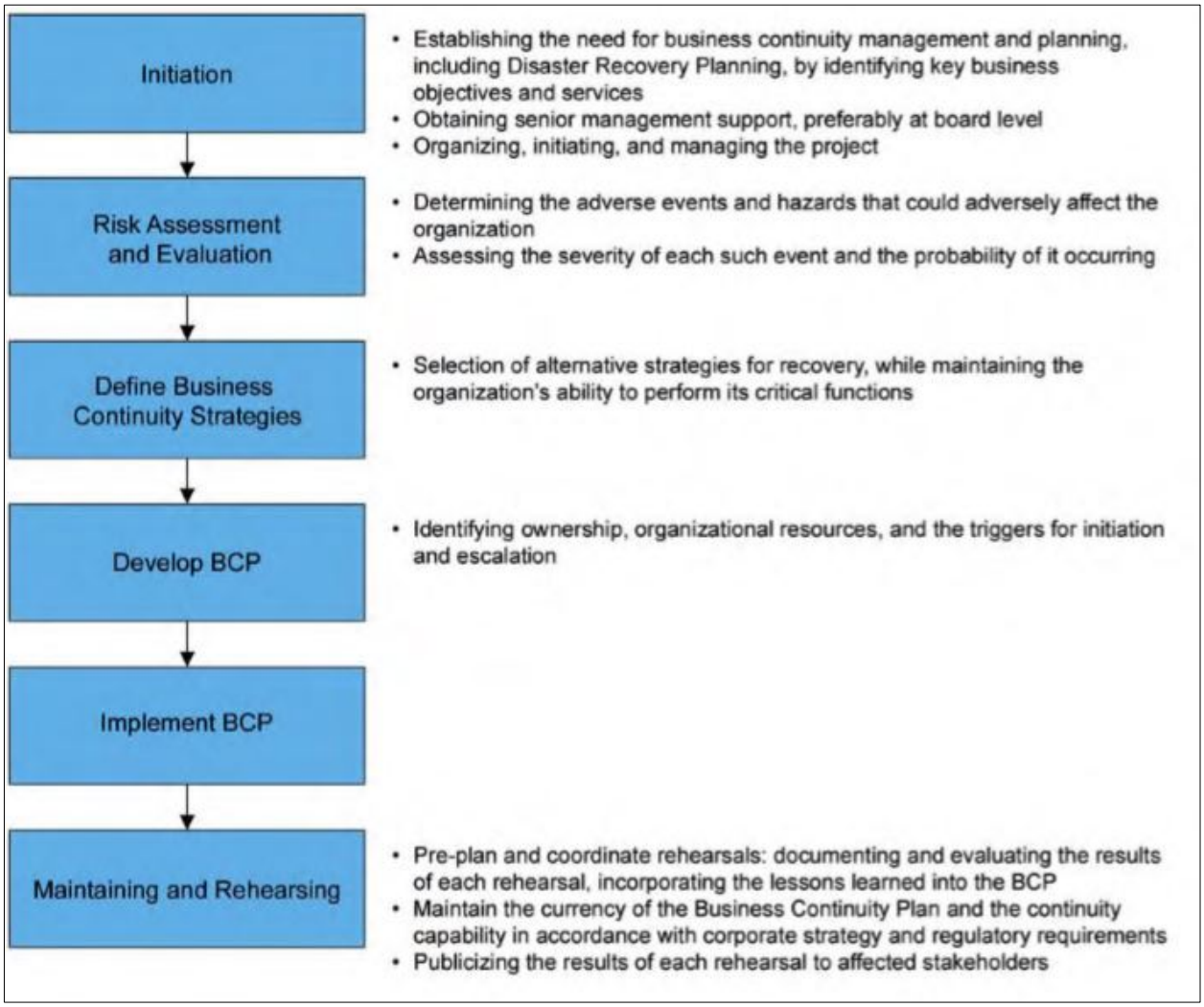

Image 1. Business Continuity Plan implementation process.

One critical component is to have a document hierarchy that enables a risk-based approach. The document hierarchy requires are described in Table 1.

Table 1

Document	Short description
Validation Policy	The validation policy is a high-level document describing the requirements for a risk-based validation program.
Computer Validation Standard	The validation standard is a document that describes the specific requirements for the risk-based computer validation program.
Computer Validation Procedures	The computer validation procedure is a document that describes the specific steps to validate computer systems based on their level of risk. The procedure translates standard requirements into “how to” actions that promote a risk-based approach.

Risk assessments are a critical activity needed to enable a risk-based computer validation approach. The following risk assessments are needed:

- System-Level Risk Assessment
- Requirement Risk Assessment
- The system-level risk assessment is intended to determine whether the system is high, medium, or low risk. This assessment should determine the system risk impact to the following:
- Product Quality
- Patient Safety
- Compliance
- Safety
- Business Process
- Complexity.

The system-level risk assessment is an input to the risk-based computer validation strategy. The outcome of the system-level risk assessment should support a risk-based validation approach.

The outcome of the system-level risk assessment should enable the following approach:

- High-risk systems should require a more stringent validation effort;
- Medium-risk systems should require a less stringent approach than high-risk systems;
- Low-risk systems should require a much less stringent approach than medium risk systems.

Procedures should clearly describe the required validation deliverables for each risk level. High-risk systems should have more testing and validation deliverables. Medium or low-risk systems should require less testing of non-critical, low-risk requirements. For medium or low-risk systems, procedures should allow combining documents and integrating validation activities.

Requirements risk assessments are intended determine whether individual requirements are high, medium or low risk.

High-risk systems should require testing all high and medium-risk requirements. High-risk systems should require testing a sampling of low-risk requirements. Medium-risk requirements should require testing all high- risk requirements with a sampling of critical medium and low-risk requirements. Low-risk systems should require testing only critical high-risk requirements and sampling medium requirements.

These risk assessments will facilitate an objective risk-based computer validation approach. The output of these assessments is critical to the validation strategy.

The system-level risk assessment is an input to the risk-based computer validation strategy. The outcome of the system-level risk assessment should support a risk-based validation approach.

An information technology (IT) disaster recovery plan (DRP) should be developed in conjunction with the BCP. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

IT Recovery Strategies. Recovery strategies should be developed for IT systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the “system,” the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.).
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals).
- Connectivity to a service provider (fiber, cable, wireless, etc.).
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.).
- Data and restoration.

Some business applications cannot tolerate any downtime. They utilize dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. Only larger companies can afford this very expensive solution. However, there are other solutions available for small to medium sized businesses with critical business applications and data to protect.

Developing an IT DRP. Businesses should develop an IT DRP. It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up. Identify critical software applications, data, and hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration. Document the IT DRP as part of the BCP. Test the plan periodically to make sure that it works.

Data Backup. Businesses generate large amounts of data and data files are changing throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data could result in significant business disruption. Data backup and recovery should be an integral part of the BCP and information technology DRP. Developing a data backup strategy begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan. Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server can then be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Options for Data Backup. Tapes, cartridges and large capacity USB drives with integrated data backup software are effective means for businesses to backup data. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan. Backups should be stored with the same level of security as the original data. Many vendors offer online data backup services including storage in the “cloud”. This is a cost-effective solution for businesses with an internet connection. Software installed on the client server or computer is automatically backed up. Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business. The business impact analysis should evaluate the potential for lost data and define the “recovery point objective.” Data restoration times should be confirmed and compared with the IT and business function recovery time objectives.

Conclusion. In order to implement a computer validation risk-based program, an appropriate document hierarchy is needed. Validation policies, standards, and procedures must be created or revised to enable a risk-based approach. System level and requirements risk assessments are a critical component of a risk-based approach for computer validation.