IT controls for ‘infrastructure as a service’ in the biopharmaceutical industry

BioPhorum Compliance Workstream
24 April 2018

Rekha Alaguchellappan	BMS
Jodi Dey	Pfizer
Steve Atkinson	BioPhorum

CONNECT
COLLABORATE
ACCELERATE™

Agenda

- What is BioPhorum?
- IT controls for ‘infrastructure as a service’ in the biopharmaceutical industry paper
- Publications and next steps

BioPhorum mission

To create an environment where the global biopharmaceutical industry can collaborate and accelerate their rate of progress, for the benefit of all

BioPhorum IT (BPIT)

- **established January 2016, focused on digital transformation in the pharma manufacturing domain**
- **aims to share best practices, to collaborate on common challenges and problem solving through deliverables-driven work streams**
- **proactively addresses key regulatory issues within priority focus areas**
- **provides a single voice to suppliers, regulatory bodies and other key stakeholders, to further the needs of the industry**

IT controls for ‘infrastructure as a service’ in the biopharmaceutical industry

Authors

Cynthia Fliszar	Pfizer
Horst Froede	Roche
Jodi Dey	Pfizer
Rekha Alaguchellappan	BMS
Steve Atkinson	BioPhorum

Background

- companies are increasingly moving towards using the cloud to provide external hosting
- driven by cost, speed and flexibility
- compliance concerns within the biopharmaceutical industry toward this approach
- relative controls responsibilities between the provider and customer were unclear
- interest from the cloud providers for a clear and consistent approach to regulatory compliance and reduce the number of queries from customers and requests for audits

Paper purpose and approach

Purpose

- to describe the IT controls required for leveraging the ‘infrastructure as a service’ (IaaS) model and how these controls will need to be implemented as a shared responsibility between the cloud service provider (CSP) and the customer using the service

Approach

- small team was convened to develop the paper using the broader compliance workstream to review the developing document

- during the development of the paper the team leveraged the knowledge and experience from within their companies

Scope of the paper

- the scope is IaaS with the focus being on the shared nature of the IT control responsibilities between the customer and the cloud service provider (CSP)

- it does not include ‘platform as a service’ (PaaS) or ‘software as a service’ (SaaS). The guidelines provided in this document are appropriate for all IaaS providers

- the team decided to focus particularly on IaaS given this is where current business interest resides. It may be appropriate to extend the scope to PaaS and SaaS in the future

- areas covered in the paper remain relevant for PaaS and SaaS. However, where the line is drawn between CSP and customer responsibilities would be different

Cloud service models

The National Institute of Standards and Technology's definition of ‘cloud computing’ defines the different service models as:

- **Infrastructure as a Service (IaaS)**: the capability provided to the consumer is for the processing, storage, networking and other fundamental computing resources where the consumer can deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but does control operating systems, storage and deployed applications; and possibly has limited control of selected networking components (e.g. host firewalls)

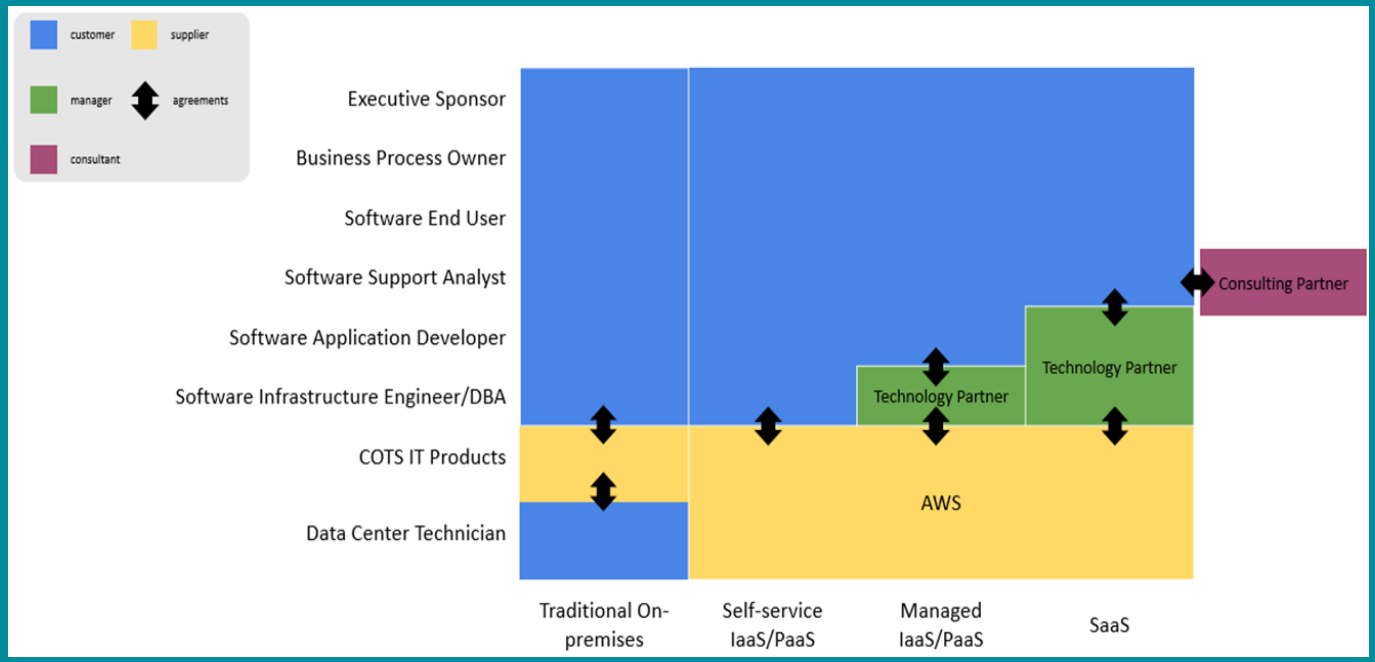
- **Platform as a Service (PaaS)**: the capability provided to the consumer is for deploying, onto the cloud infrastructure, consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including networks, servers, operating systems or storage) but has control over the deployed applications and possibly the configuration settings for the application-hosting environment

- **Software as a Service (SaaS)**: the capability provided to the consumer is for using the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure (including networks, servers, operating systems or storage) or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

CSP Models

Although the scope of this document is specific to IaaS, it is important to understand the different responsibility models of CSPs compared to traditional on-premises IT. Each of these models has a unique set of shared responsibilities and formal agreements.

The figure below compares traditional IT responsibilities and agreements with the CSP's IaaS, PaaS and SaaS cloud models.



Roles and responsibilities

- the document clarifies the shared responsibilities between the CSP and the customer, and helps identify key customer actions that may be required to ensure a GxP compliant solution in the IaaS cloud

- customer internal policies and procedures must be reviewed and revised (as necessary) to reflect the usage of CSP for regulatory purposes. These steps will help in the transition to cloud while maintaining a manageable, secure, regulatory-compliant and policy-compliant environment

- customers should discuss the extent and manner in which they want to leverage cloud services both in their business generally and in the context of GxP activities. It is recommended that the customer creates an overall governance body that can oversee the cloud strategy and monitor key factors such as cost, risk and regulatory exposure

IT controls for ‘infrastructure as a service’

- access management
- audit trail/logging
- back up
- business continuity management
- change management
- disaster recovery
- document management
- event/Incident management
- periodic review
- policies and procedures
- problem management
- qualification
- quality assurance
- quality management system
- risk assessment
- security management
- service asset/configuration management
- service provider/ supplier management
- training
- validation

IT controls checklist - examples

For each control area listed there is a checklist that can be used to ensure clarity of responsibilities between the CSP and the customers. This list is not exhaustive but provides a strong basis for discussion between the CSP and an internal IT team.

Access Management

Control area	CSP checklist	Customer checklist
Access management **Definition** : The process for allowing users to use IT services, data or other assets. It helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorized users can access or modify them. Access management implements an organization's information management security and is sometimes referred to as 'rights management' or 'identity management'.	• how does the provider manage access privileges to the internal network? Do they use the concept of 'least privilege'? • does all provider user access require documented approval from authorized personnel? • how is physical access to the data centers controlled? • how is tailgating on access controlled? • are access lists to data centers and devices reviewed regularly? • are access rights revoked immediately when no longer required? • are inactive user accounts revoked? how regularly are these reviewed?	• does the CSP provide services to configure the use of, and access to, the cloud service? • how does the customer configure access to its data and accounts? Does the customer have full control of this configuration?

IT controls examples (continued)

Business Continuity Management

Control area	CSP checklist	Customer checklist
Business continuity management **Definition**: The process for managing risks that could seriously affect the business. It safeguards the interests of key stakeholders and an organization's reputation, brand and value-creating activities.	• how does the provider ensure any system or hardware failures have minimal impact on the customer? • who is responsible for business continuity management in the provider organization? • how is the infrastructure configured to minimize the customer impact of a failure? • are data centers located in low-risk geographical areas? • how does the provider ensure uninterrupted power supplies? • who checks the resiliency plans within the provider organization?	• does the customer have a robust continuity plan, including utilization of frequent server instance backups and the flexibility to place instances and store data within and across regions? • does the customer have the ability to architect their usage across regions and availability zones?

IT Controls checklist – examples (continued)

Event/incident management

Control area	CSP checklist	Customer checklist
Event/incident management **Definition:** The process that monitors all events that occur within the IT infrastructure. It allows for normal operation and also detects and escalates exception conditions.	• Does the provider have a formal, documented incident response policy and program? • How does the provider identify early those issues that may impact on customers? • What are the incident criteria used? • Are incident roles and responsibilities documented and understood? • How are customers notified of an incident? • Is a post mortem undertaken after an incident? Who reviews the outcomes and are the actions captured and assigned? • Is the provider's incident management approach reviewed by internal or external auditors?	• Does the customer have established incident response and event management procedures to quickly detect security events? • Is it clear to the customer how to notify the provider in the event of an incident?

IT controls checklist examples (continued)

Validation

Control area	CSP checklist	Customer checklist
Validation **Definition:** The method for establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product that meets its pre-determined specifications and quality attributes.	• does the provider utilize commercially available infrastructure software products that are developed and tested to IT industry standards (e.g. SOC, ISO, PCI, etc.)? • how does the provider ensure that key controls have been implemented, including those over the installation and operation of product components, product changes, risk management, security management of information availability, integrity and confidentiality, and data protection – backup, restore and archiving?	• does the customer have a process for configuring and operating cloud services to meet their data-, application- and industry-specific needs, such as GxP software validation and GxP infrastructure qualification?

Customer considerations

• when implementing a cloud service, the onus is on the customer to ensure that the shared responsibility model defined in this document is current

• they should assess whether these controls are sufficient to meet their regulatory and business needs

• include any other considerations to achieve a compliant implementation of the cloud service

Supplementary customer considerations

This document is focused on the defined IT controls. However, there might be additional regulatory and/or legal requirements that may have to be taken into consideration when establishing cloud services. These requirements might include, but are not limited to, these areas:

- regulators expectations are that the customer has to audit the CSP. You will need to check with your CSP whether they support individual customer audits.
- the CSP may provide reports from standard audits performed by independent auditors, which can be used to demonstrate the robustness of their quality management service
- the customer is responsible for understanding any legal/regulatory requirements about the country in which the customer's data is stored (e.g. for data transfer agreements)
- some vendors may provide the ability for the customer to control the location of data by country but internal security protocols may not permit disclosure of data center street addresses
- regulators expect that GxP quality systems have an independent quality assurance function. Customers must understand that with some providers the quality assurance function is integrated within the security function
- customers are responsible for subscribing to any CSP communications to determine the impact of any changes in their environment

Conclusion

- the use of cloud services has increased in recent years and continues to do so, giving cost benefits and flexibility to quickly expand or contract services as business requirements change

- with increased usage comes the need to ensure that compliance concerns are alleviated through increased transparency and clarity on the relative provider and customer responsibilities

- the paper provides guidance to use IaaS with increased confidence

- there are areas that may require further discussion and clarity

- through the work of BPIT there is recognition that using the cloud for IaaS can provide the business benefits expected while ensuring regulatory compliance

Cloud provider response to the paper

Amazon Web Services (AWS)

- discussions have taken place over recent months
- AWS have provided responses to the questions in each session
- AWS have committed to formally publishing a paper in response to the BioPhorum paper shortly

Microsoft

- initial discussions have taken place
- Microsoft have committed to responding to the paper
- discussions will continue over the next few weeks and months

Next steps

- socialize the IT Controls for the ‘IaaS’ paper within each BPIT member company
- progress responses to the paper with Amazon Web Services and Microsoft
- potentially look to extend the paper to include controls approach for PaaS and SaaS

BPIT member companies quotes on usefulness of Cloud paper

use as reference document to support audits/inspections

use as basis for AWS Cloud Controls responsibility document

supports and provides assurance for ‘cloud first’ approach

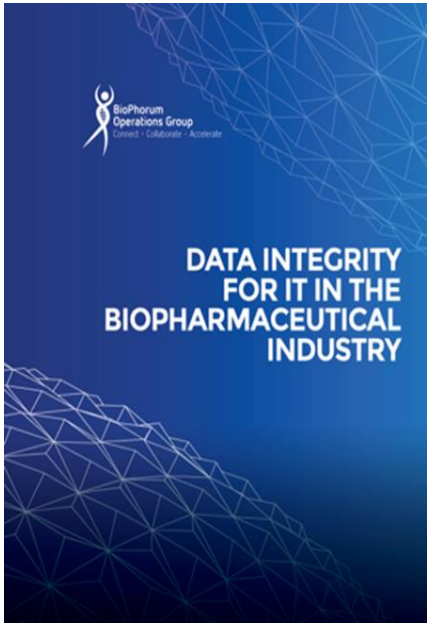
use document to change internal mind set on cloud utilization

will look to use the template for cloud providers

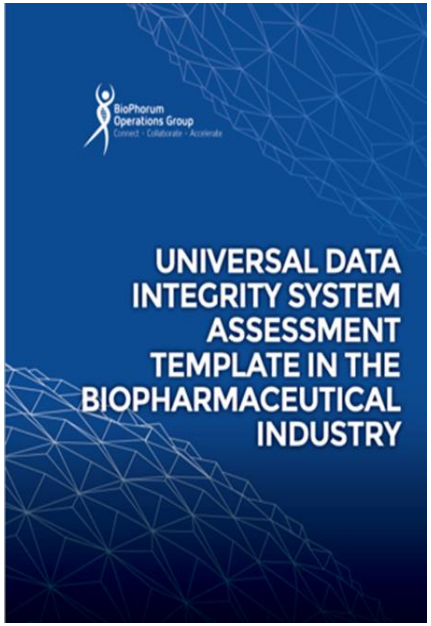
Publication

https://www.biophorum.com/iaas-white-paper/

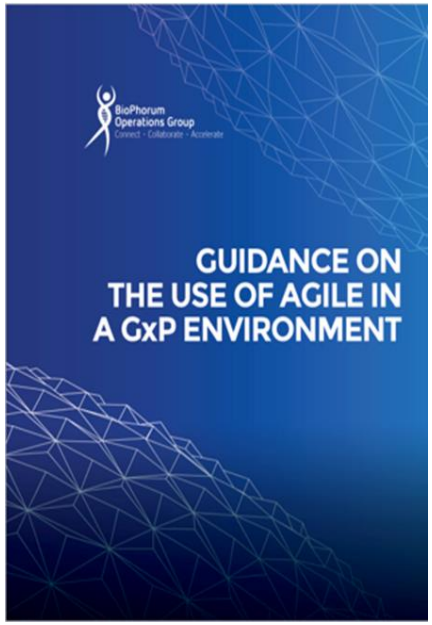
BPIT Compliance Workstream publications



www.biophorum.com/universal-data-integrity-system-assessment-template-in-the-biopharmaceutical-industry/



www.biophorum.com/data-integrity-for-it-in-the-biopharmaceutical-industry/



www.biophorum.com/data-integrity-agile-guidance/

List of controls with definitions

Access management: the process for allowing users to use IT services, data or other assets. It helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorized users can access or modify them. Access management implements an organization's information management security and is sometimes referred to as 'rights management' or 'identity management'

Audit trail/logging: a chronological record of system activities that is sufficient to enable the reconstruction, review and examination of the sequence of activities surrounding or leading to each event in the path of a transaction from its inception to output of final results

Backup: copying data to protect against the loss of integrity or availability of the original

Business continuity management: the process for managing risks that could seriously affect the business. It safeguards the interests of key stakeholders and an organization's reputation, brand and value-creating activities. The process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. Business continuity management sets the objectives, scope and requirements for IT service continuity management

Change management: the process for controlling the lifecycle of all changes, enabling changes to be made with minimum disruption to IT services

Disaster recovery: returning a configuration item or an IT service to a working state. Recovery of an IT service often includes recovering data to a known consistent state. After recovery, further steps may be needed before the IT service can be made available to the users (restoration)

List of controls with definitions (continued)

Risk assessment: the process for identifying, assessing and controlling risks. The phrase ‘risk management’ is sometimes used to refer to the second part of the overall process after risks have been identified and assessed, i.e. ‘risk assessment and management’

Security management: a set of tools, data and information that is used to support information security management.

Service asset and configuration management: the process for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between them

Service provider/supplier management: the process for obtaining value for money from service providers/suppliers, ensuring that all contracts and agreements support the needs of the business and that all service providers/suppliers meet their contractual commitments

Training: the process of teaching any skills and knowledge that relate to specific competencies. Training has the specific goals of improving one's capability, capacity, productivity and performance

Validation: the method for establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product that meets its pre-determined specifications and quality attributes.

List of controls with definitions (continued)

Document management: the process by which an organization stores, manages and tracks its electronic documents

Event/incident management: the process that monitors all events that occur within the IT infrastructure. It allows for normal operation and also detects and escalates exception conditions

Periodic review: a recorded assessment of the documentation, procedures, records and performance of a computer system to determine whether it is still in a validated state and what actions, if any, are necessary to restore its validated state. The frequency of review depends on a system's complexity, criticality and rate of change

Policies and procedures: the formally documented management expectations and intentions. Policies are used to direct decisions and ensure the consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure, etc.

Problem management: the process for managing the lifecycle of all problems. It proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented

Qualification: the process of demonstrating whether an entity is capable of fulfilling its specified requirements. In the context of meeting regulatory requirements, 'qualification' implies adherence to strict documentation requirements, reviews and approvals

Quality management system: the framework of policies, processes, functions, standards, guidelines and tools that ensures an organization is of a suitable quality to reliably meet business objectives or service levels (including internal audits)

Quality assurance: the practice for ensuring that the quality of a service, process or other service asset will provide its intended value. The phrase 'quality assurance' is also used to refer to a function or team that performs this role

Anti-Trust Compliance Statement v4.0

It is the clear policy of BioPhorum that Biophorum and its members will comply with all relevant anti-trust laws in all relevant jurisdictions.

All BioPhorum meetings and activities shall be conducted to strictly abide by all applicable antitrust laws. Meetings attended by BioPhorum members are not to be used to discuss prices, promotions, refusals to deal, boycotts, terms and conditions of sale, market assignments, confidential business plans or other subjects that could restrain competition.

Anti-trust violations may be alleged on the basis of the mere appearance of unlawful activity. For example, discussion of a sensitive topic, such as price, followed by parallel action by those involved or present at the discussion, may be sufficient to infer price-fixing activity and thus lead to investigations by the relevant authorities.

Criminal prosecution by federal or state authorities is a very real possibility for violations of the antitrust laws. Imprisonment, fines or treble damages may ensue. BioPhorum, its members and guests must conduct themselves in a manner that avoids even the perception or slightest suspicion that antitrust laws are being violated. Whenever uncertainty exists as to the legality of conduct, obtain legal advice. If, during any meeting, you are uncomfortable with or questions arise regarding the direction of a discussion, stop the discussion, excuse yourself and then promptly consult with counsel.

The antitrust laws do not prohibit all meetings and discussions between competitors, especially when the purpose is to strengthen competition and improve the working and efficiency of the marketplace. It is in this spirit that the BioPhorum conducts its meetings and conferences.

Supplier Interactions Policy v3.0

The BioPhorum Operations Group (BPOG) facilitates a cross industry collaboration process for Biopharmaceutical developers and manufacturers with the aim of accelerating the rate at which the biopharma industry attains a mature and lean state benefitting patients and stakeholders alike. Collaboration modes include best practice sharing, benchmarking, joint-solution development to common challenges, definition of standards requirements and formation of collective perspectives to mutual opportunities and regulatory guidelines.

Biopharmaceutical developers and manufacturers recognize the legally enforceable duties they have including the responsibility to control the quality of materials from their suppliers. From time to time BPOG-facilitated collaboration requires, and benefits from, supplier interaction.

Suppliers are providers of supply chain materials such as chemicals, glass, components, excipients, and media. They are also providers of process equipment such as single use systems, engineering parts and consumables. BPOG-facilitated supplier interactions may involve: harmonizing manufacturer requirements and communicating these to suppliers; seeking feedback on proposed standards; gaining opinions and ideas related to business process improvement; use of problem solving tools; and gaining support for new ways of working.

The ultimate goal of the BPOG collaboration is to strengthen competition, assure product quality and protect patient supply.

The purpose of this document is to set out the principles and policies that BPOG follows to ensure that BPOG-facilitated supplier interactions are conducted in the correct and appropriate way to meet all legal and business compliance requirements.

Underlying Principles and Policies

Competition Laws

All supplier interactions will comply with anti trust and competition laws and have regard to BPOG's anti-trust compliance statement

Member responsibilities

Individual biopharma companies are responsible for defining their requirements of suppliers.

Innovation and commercial interests

All supplier interactions will recognise and respect the need for suppliers to innovate and pursue their own commercial interests.

Intellectual Property

All supplier interactions will respect suppliers' intellectual property rights.

Confidentiality / Non Disclosure

All supplier interactions will take into account, respect and encourage compliance with confidentiality and non-disclosure agreements.

Equal Treatment

All suppliers will be treated equally

Communication

These principles, policies and procedures will be communicated to BPOG members and suppliers whenever supplier interactions are planned or are taking place.

BPOG responsibilities

- It is the responsibility of BPOG Directors to ensure that these principles and policies are upheld and procedures are in place to support them.
- BPOG will educate and train its staff so they understand and follow these principles and policies and are able to communicate them when needed.
- BPOG documentation will reference or directly include relevant parts of the Supplier Interaction Policy.
- BPOG will establish and maintain records to demonstrate compliance with these principles and policies.

Code of Conduct – BPOG information sharing v2.0

Introduction

The BioPhorum Operations Group (BPOG) is a cross industry collaboration with the aim of sharing best practice in the area of Operational Excellence.

Participation in BPOG is restricted to authorized member company representatives as described in the Principles of Membership Agreement.

While sharing information is central to the process of this collaboration, it is important to understand what information is appropriate to share. Our companies have a great deal of confidential information and intellectual property that should not be shared within BPOG.

This document seeks to guide the reader so that the individuals and companies involved follow the correct code of conduct and problems are avoided.

It is the clear and stated intention of BPOG that the Group and its activities are conducted at all times in full compliance with relevant completion/anti-trust rules.

Responsibilities

It is the responsibility of every person who participates in a BPOG event or sharing activity to make sure they are aware of what information is appropriate to share. Furthermore, all participants are responsible for vetting any information to be shared via their company's public disclosure review processes and that all information shared is free of any "Confidential" stamps or markings.

The key contact (L2) for each member company should ensure confidentiality and that IP issues are highlighted to their colleagues and all applicable company policies regarding external collaboration and public disclosure are adhered to.

The BPOG facilitators are responsible for reminding all participants of their obligations with respect to information sharing.

Sharing information

The following list is representative of the types of disclosures commonly allowed by corporate policies. BPOG participants should review their company policies to ensure they are in compliance prior to any disclosures. Information in the following areas is typically allowed:

- Operational excellence best practice models
- Management approaches and philosophies
- Organizing and planning ways of working
- Non-product or process specific generic operating procedures
- Information in the public domain
- Information provided by suppliers which would ordinarily be shared with customers
- Non-product or process specific generic engineering or technical information relating to process equipment
- General learning and 'context' conclusions from QA and Regulatory activity

Information from the following areas is typically prohibited by corporate policies

- Product related information
- Product related process data which constitutes intellectual property
- Specific audit or regulatory inspection findings or observations
- Product specific analytical methods
- Specific cost numbers where a market advantage may result or a supplier might be disadvantaged
- Information that is marked as confidential by the member company or a supplier
- Price information of any type
- Proprietary information including intellectual property and patented processes and equipment

BPOG event participants should direct all questions regarding information disclosure to their L2 BPOG representatives or corporate legal departments.