PRE-SALES REQUIREMENTS ASSESSMENT QUESTIONNAIRE

This document is designed to help you assess your client's compliance requirements, which in turn can help you prepare a strong presentation for your Microsoft Dynamics™ GP solution.

This questionnaire is organized into four sections:

1) Client Organization

2) Audit Trails

3) Electronic Signatures

4) System Requirements

Appendix A includes a Glossary of Terms.

Question Area	Explanation/Drill-Down	Solution
Client Organization:		
Is your organization required to comply with regulations that govern how you must control and manage your business data?	Life Sciences -21 CFR Part 11 Publicly Traded -Sarbanes Oxley Healthcare -HIPAA, JCAHO Public Sector -FISMA	**Audit Trails** and **Electronic Signatures for Microsoft Dynamics GP** increase the data integrity and data control of your business systems. They are designed to meet the needs of organizations that must comply with regulatory requirements for how their data is obtained, used, managed, and secured.
Do these regulations require the ability to re-create change history associated with certain business processes?	Regulations will typically require tracking and auditing for specific system changes, such as changes supporting business processes that pose risk if performed incorrectly.	**Audit Trails** may be activated on just those areas of the system that are required by the customer. This keeps the audit database uncluttered and manageable in size. It also enables easy reporting on change history.
According to the regulations you must comply with, what business processes must have controls placed on them at the business systems level (i.e. change history tracked, preventative controls enabled)? **Can you give me some examples?**	Most regulations set criteria for which business processes must have change history tracked and preventative controls applied. For FDA regulated firms, these business processes are called 'significant processes'. For Sarbanes-Oxley compliance, these business processes are deemed 'risk processes'.	**Audit Trails** may be activated on just those areas of the system that are required by the customer. This keeps the audit database uncluttered and manageable in size. It also enables easy reporting on change history. Other auditing tools are often only enabled at the database level and not at the application level. This creates a huge amount of change and audit data that must be tracked and managed, and makes it difficult to reassemble the history of changes associated with a business process.

PRE-SALES REQUIREMENTS ASSESSMENT QUESTIONNAIRE

Question Area	Explanation/Drill-Down	Solution
Audit Trails:		
What change history information does your compliance program require you to track? **Are you required to track not only the change, but the user, time and date stamp, and the before-change and after-change data values associated with the change? Is it important that the change not obscure previously recorded information?**	Example: If vendor pay-to address was changed, regulations will require the ability to see real-time, data, user, and vendor pay-to address both before the change and after the change. If it was changed multiple times, the regulations (and auditors enforcing the regulations) will want to see the change history going back over time.	Regulations will typically require time, date, user, and before-change and after-change data values to be tracked in a way that makes it easy to reassemble the change history. **Audit Trails** provides this capability. Most alternate approaches do not provide this capability. They might capture information about the transaction, but not the specific before-change and after-change data values. If they do track the change, the information might not be captured in a structured manner that allows the change history to be easily reassembled.
What systems and processes are you using today to support regulatory compliance requirements?	Many clients are currently working with compliance processes via manual or paper-based methods — even if they are working with Microsoft Office Word and Microsoft Office Excel®. We should help the client understand that when compliance processes don't occur automatically within the system, hours are lost performing manual tasks, the risk of errors increases, and reporting information is difficult to unify and quantify.	Once **Audit Trails** is set up, audit trails happen automatically and in the background. Users can perform business processes efficiently using Microsoft Dynamics GP, without having to stop to manually capture change history or enforce paper-based controls.
Are you required to store and to retrieve the audit database in offline and online formats, while enforcing strong security controls? **Does the audit trail need to support scheduled system maintenance and archival procedures?** **Does the audit trail documentation need to be retained for a specific length of time?**	Most regulations specify that change history be maintained in both offline and online formats for a specified number of years. Regulations also require that information can be retrieved in a timely manner should the need arise. Regulatory auditors will routinely ask to see this information and understand the client's ability to produce it in a timely manner.	**Audit Trails** stores change history information in a separate database rather than in the Microsoft Dynamics GP production database. As a result, clients are able to implement strong controls and procedures around online and offline storage of the data. This is an important differentiator for **Audit Trails** for Microsoft Dynamics GP when compared to other auditing tools. **Audit Trails** also provides screen-based functionality for defining the audit database and moving it to offline storage. This reduces the time and potential error associated with this process.

Microsoft

PRE-SALES REQUIREMENTS ASSESSMENT QUESTIONNAIRE

Question Area	Explanation/Drill-Down	Solution
Audit Trails:		
If data changes occur at the Microsoft SQL Server™ database level, rather than through Microsoft Dynamics GP, are you required to track those data changes?	This refers to controlling access and protecting the integrity of the data at the application level and at the level of the underlying database. Regulations require both. For example, if a fraud were to be perpetrated in the software application, and then data changed directly through accessing the tables in the production Microsoft SQL Server database as an effort to cover the fraud, **Audit Trails** will capture change history for all of these changes. This change history resides in a separate database that may have higher levels of security and access prevention than the Microsoft Dynamics GP production database itself.	**Audit Trails** captures changes made at the application level and at the database level. This capability differentiates **Audit Trails** for Microsoft Dynamics GP from audit tools that work just within the application layer, or just at the database level.
Electronic Signatures:		
Are there points in your business processes that require preventative controls to prohibit unauthorized changes from taking place?	Preventative controls require completion of an approval step before a change is allowed to take place in a system. Credit Holds is an example of a preventative control that is standard in Microsoft Dynamics GP. Many companies require other preventative controls that are specific to their business.	**Electronic Signatures** offers preventative controls that can be applied at any point within the system. With **Electronic Signatures**, the user receives a pop-up window that requires authorization information to be entered before they may proceed. Authorization information may include one or more passwords, reason codes, and notes related to the change.
Do you require multiple authorized signatures before changes controlled by Electronic Signatures are allowed to take place?	Many regulations require the capture of two or more authorized signatures before a change is allowed to take place.	**Electronic Signatures** tracks authorized signers specific to the control point, and enables use of one or more electronic signatures for approval.
Can you give me an example of a business process in your organization that would require this type of preventative control?	These are typically tasks and activities that, if performed incorrectly, could result in a significant loss (human harm or death, financial reporting discrepancy, financial malfeasance, and so on).	Use a specific, relevant business process during your solution presentation as a means to illustrate the value of **Electronic Signatures** to the client's organization. Demonstrate that **Electronic Signatures** is flexible enough to meet a range of preventative control needs.

Microsoft

PRE-SALES REQUIREMENTS ASSESSMENT QUESTIONNAIRE

Question Area	Explanation/Drill-Down	Solution
Electronic Signatures:		
Do you require authorized signers to complete electronic signature requests from remote locations?	If no authorized signers are physically present at the same location as the initiator of the electronic signature, it can delay the approval process.	**Electronic Signatures** supports remote authorization. An authorized signer can receive notification that an electronic signature requires approval, and also can send system notifications to approve the electronic signature.
Is it important to capture change history information when these electronic authorizations occur?	Most regulations require authorization at the point of the change (versus prior to or after the actual system change). Some organizations may also require capture of information about the change, such as reason codes.	**Electronic Signatures** supports capture of authorization information at the time of the change. **Electronic Signatures** supports the capture of reason codes and notes, along with authorized signer information.
System Requirements:		
What version of Microsoft Dynamics GP will you be using?	Microsoft Business Solutions–Great Plains 8.0 (now part of Microsoft Dynamics), Microsoft Dynamics GP 9.0, or Microsoft Dynamics GP 10.0?	**Audit Trails** and **Electronic Signatures** are available for all three versions.
How many company databases within Microsoft Dynamics GP might house Audit Trails and/or Electronic Signatures?	Learn the client's level of use for multiple databases within Microsoft Dynamics GP.	This information will help you understand the scope of deployment for Microsoft Dynamics GP and the value impact that **Audit Trails** and **Electronic Signatures** can have on the client's organization.
How many different fields or tables could you see being audited within your system?	Get the client's view of the number of places in the system where they will apply audit trails.	This information will help you understand the scope and the value impact that **Audit Trails** can have on the client's organization.
How many different points in the system would you envision needing preventative controls, such as electronic signatures, being applied?	Learn the number of places within Microsoft Dynamics GP that the client envisions needing preventative controls.	This information will help you understand the scope and the value impact that **Electronic Signatures** can have on the client's organization.
What types of users do you envision having access to audit trails information? How many different user profiles would they fall into?	User profiles are considered when designing and deploying **Audit Trails**.	**Audit Trails** enables the setup of user profiles for access to audit information. Then, during setup and administration, the client points users to user profiles. In this way, the system is able to restrict user access to certain **Audit Trails** information according to a user's profile.
How many employees or employee groups will need to view the audit trails reports?	Learn about the client's reporting needs, and the number of different users that may require reporting access.	This information will help you understand the scope and the value impact that **Audit Trails** can have on the client's organization.

PRE-SALES REQUIREMENTS ASSESSMENT QUESTIONNAIRE

Appendix A: Glossary of Terms

21 CFR Part 11: A Food and Drug Administration (FDA) regulation that applies to certain products that may cause harm or death to humans if produced or distributed incorrectly. Companies that fall under this regulation include pharmaceutical, biotechnology, medical device, and biologic companies. Section 21 of the Code of Federal Regulations, Part 11 addresses electronic record keeping—in specific, the controls, processes, and capabilities that must be in place for a company to operate with electronic, versus manual, records.

Change data values: The before-change data value refers to the information that existed before a change was completed. After-change data value refers to the information after the change was completed.

Compliance program: For most compliance regulations, each company must establish its own compliance program. This will include what they will track and control and how they will do it in accordance with their interpretation of the regulation. The company chooses a point on the compliance risk versus cost curve, with the goal of maximizing their risk containment versus cost for compliance. Ultimately, a company must be able to defend the design of their compliance program, and prove that they operated in accordance with the controls specified.

Electronic signature: A form of electronic authorization based on strong passwords.

FISMA: The Federal Information Security Management Act requires agency management accountability for the security program and adherence to the National Institute of Standards and Technology (NIST) requirements for computer security.

HHS-OIG: The Department of Health & Human Services, Office of the Inspector General publishes the Fraud Prevention & Detection Compliance Guidance as an outline for an effective compliance program that must be adopted by a healthcare organization. HHS-OIG is concerned with detecting fraud in areas such as patient billing, and includes specific data management guidance that healthcare organizations must follow.

HIPAA: The Health Insurance Portability and Accountability Act is a law passed in 1996 to protect the information privacy rights of medical patients. HIPAA includes specific requirements for how a health care organization must store, manage and provide access to patient information.

JCAHO: The Joint Commission on Accreditation of Health Care Organizations is the nation's leading standards-setting and accrediting body in health care, focused on improving the quality and safety of care provided by health care organizations.

Risk process: The term used in Sarbanes-Oxley compliance for a business process that, if performed incorrectly, could result in financial harm or malfeasance. This term is used in Sarbanes-Oxley compliance to identify a business process that requires data controls.

Sarbanes-Oxley: A Federal law enacted in 2002 to increase the quality of financial reporting and the confidence of investors. The law requires publicly held companies to report accurate financial statements to shareholders, and holds company officers directly responsible for failure to do so. In addition, the Sarbanes-Oxley Act specifies levels of control and security that must be implemented to ensure accurate data, as well as the ability to recreate change history in financial processes to investigate potential wrong-doing. Finally, the Sarbanes-Oxley Act specifies levels of information transparency, including time periods within which publicly held companies must act to share material changes in their business.

Significant process: The term used in FDA compliance for a business process that, if performed incorrectly, could result in harm or death to humans. This term is used by the FDA to identify a business process that requires data controls.

Strong password: A type of password with characteristics that would make it unlikely to be discovered for unauthorized use. A password is considered strong if it is minimally 8 characters in length, consists of alpha and numeric values, case sensitive, and has enforced time-change intervals and repeat-frequency controls. A strong password should also not be allowed to be the same value as the user ID.