WHITE PAPER

E-SHARE – A NON-INTRUSIVE SOLUTION FOR FILE SHARING AND CONTENT COLLABORATON IN LIFE SCIENCES

Introduction – Modern Software in Regulated Environments

In modern business, the use of automation via software solutions is universal. Software is leveraged in every business, in one capacity or another, to increase productivity and efficiency of various business workloads. For businesses that operate under heavy regulation, computer systems come under the scrutiny of regulation in the form of demand for assurance that these systems operate with a certain degree of assurance that they will consistently meet a set of predetermined requirements. Such requirements are especially rigorous in the Life Sciences industry where these systems may have an impact on product quality, safety or efficacy, or if the system is used to support regulatory submission functions.

In these highly regulated environments, where system qualification and validation are common practice, it is easy to fall into the practice of applying the same level of rigor for all systems and software. However, not all systems and software are created equally and overapplying these requirements can unnecessarily increase cost, decrease efficiency and impact the utility of solutions that fall outside of the actual intent and requirement of the regulations.

The rate of changes, updates and patches associated with the use of modern software challenge the ability to follow a system validation protocol for all systems. Additionally, the paradigm shift from traditional local installation of software to Software-as-a-Service (SaaS) solutions, that are installed elsewhere and delivered over the internet, has become a forcing function toward differentiating classes of systems and which may need to be validated versus qualified. This has driven broader adoption of a risk-based approach to how systems are classified to focus validation efforts on the systems closest to the critical path that pose the highest risk in the event of malfunction.

A risk-based approach to system validation was proposed in Good Automation Manufacturing Process (GAMP) version 5. The approach aims to ensure that validation effort is proportionate to the criticality of the system functionalities, and those with the highest risk receive the most concentrated validation effort. Ultimately, the extent of validation is determined by the risk a specific computer system or functionality can have on data integrity, product quality and safety. The assessment of risk consists of a set of questions.

- Risk Identification - What could go wrong with a given system?
- Risk Impact - What is the impact of a malfunction of the system?
- Risk Probability - What is the probability that the system will malfunction at some point?

Probability of the identified risk is measured as high, medium or low. This measure also helps to determine the potential for impact in evaluating the need for validation or qualification:

- High – Custom developed software of highly customized commercial-off-the-shelf (COTS) software
- Medium – Specific configurations associated with COTS software
- Low – Standard (non-configured) functions of COTS software

The risk-based approach also allows for classification of systems to evaluate which systems would be considered the highest risk based on criticality, complexity and uniqueness to the critical path of product quality, safety and efficacy or related to a regulatory submission. These are also measured in high, medium and low.

- High – Direct impact on data integrity, patient safety or overall product quality
- Medium – Indirect impact on data integrity, patient safety or overall product quality
- Low – No impact on data integrity, patient safety or overall product quality

The effort associated with further qualifying and validating a system should be reserved for those systems that are undeniably critical to consumer safety and product quality and efficacy. For lower risk systems, we should still expect quality and reliability. However, we can still qualify these systems by examining and understanding what is expected from the software or system and what quality assurance the vendor provides in the development and delivery of that software. By differentiating the various systems and developing appropriate levels of validation and qualification, cost can be reduced, and validation efforts can be concentrated where they will provide the greatest value and impact while continuing to take advantage of automation across the enterprise.

The e-Share Secure Collaboration Solution in the Regulated Enterprise

As discussed in depth in this document, organizations operating in highly regulated industries, such as Life Sciences, invest a great deal in the qualification of systems and the validation of the overall operating environment to ensure the integrity required by the FDA and GxP. Therefore, any system operating cooperatively with the validated environment must meet a level of quality and integrity itself. Whether Commercial-off-the-Shelf (COTS) software or Software-as-a-Service (SaaS), any system that falls outside of full validation requirements must at least demonstrate qualifications and fitness to operate in the broader system ecosystem.

e-Share's Secure Collaboration Platform offered from e-Share is designed to work cooperatively with high assurance operating environments by leveraging existing systems in a non-intrusive manner to fully preserve the integrity of the validated environment. By design, e-Share solutions only leverage existing customer infrastructure, data rules and policies. They deliver the full value associated with e-Share's Secure Collaboration Platform with zero intrusion or disruption to qualified and validated configuration. Robust collaboration is achieved without ever moving data from its secure and version controlled resting place. e-Share solutions interoperate with any storage solution

employed by the customer (Box, Google, AWS, Azure, Internal Storage) in an equally non-disruptive manner and adds maximum value to the Microsoft platform by leveraging and extending the capabilities of Office 365 and Azure from the Microsoft Modern Collaboration Architecture (MOCA).

The Secure Collaboration Platform is delivered as a SaaS solution. Services are delivered from a SOC 2 certified environment running from Microsoft's SOC 1 Type 2 and SOC 2 Type 2, and ISO/IEC 27001 and ISO/IEC 27018 certified Azure cloud. These layered qualifications and capabilities are designed to offer e-Share's services in a manner that is complementary to and compatible with 21 CFR part 11 requirements.

e-Share's customer guidance documentation can be formed into a checklist to offer compatibility with GxP Installation Qualification (IQ) processes and smoke testing for Operational Qualification (OQ). Step by step instructions are provided to feed installation checklists for:

- Setting up vanity domains
- Setting up Share-With-Me functionality
- Acquiring and deploying SSL certificates
- Configuring SAML and OpenID authentication
- Generating service accounts
- Configuring Single Sign-on
- Configuring Exchange Online and Office 365 for e-Share Secure Mail Gateway

e-Share provides everything needed to transform installation and testing into checklist documentation to assure integrity and repeatability of all processes required to implement and manage e-Share solutions alongside validated environments as a qualified COTS/SaaS solution.

Commitment to Quality

As a technology company serving public and private entities operating in highly regulated industries, e-Share must continuously work to maintain the critical balance between solution innovation, performance and availability with the necessary controls and safeguards required to properly uphold the security, privacy and integrity demands that our customers can and should expect from their partners. e-Share's application hosting operations and security practices are developed from vast, cross-industry experience and best practices designed to offer not only a mature quality system, but a refined practical application of technology and process. These practices have continuously evolved to offer our customers the peace of mind that they need as they seek ways to streamline their business leveraging e-Share solutions.

The e-Share quality system begins within the system development life cycle. Software development, cloud operations, business operations and cybersecurity work closely to ensure that a dynamic defense-in-depth and layered security approach is ever present in our solutions. All of this is invested to afford e-Share and our customers confidence and assurance, so that time can be focused on the value proposition of innovation rather than the inherent threats associated with the cloud and internet-based business.

Demonstration of e-Share's commitment to privacy, security, integrity and overall quality can be measured by a SOC 2 accreditation of the Secure Collaboration Platform SaaS operating environment in combination with the accreditations held and maintained by our hosting partners, including AICPA SOC 2, CSA STAR and ISO 9001 and 27001 to name a few.