PCI-DSS Compliance

The Payment Card Industry Data Security Standards (PCI DSS) are a set of technological, administrative and procedural rules that apply to the storage and processing of identifiable cardholder data, in order to ensure secure, standardised solutions are used across the industry and to minimise the likelihood of fraud.

Generally, any system that needs to store or process a 16-digit card number and the data associated with that number (such as customer name) falls under the remit of the standards. Furthermore, systems that store additional card data are subject to more stringent requirements.

The PCI DSS standards should be reviewed to ensure the appropriate requirements are applied for the type of data being processed.

Supporting PCI Compliance

Blue Prism contains a rich set of technological and administrative features that support solution designers in creating a PCI compliant solution. The implementation methodology and deployment framework also help to ensure the correct governance model is deployed as part of the solution to include:

- Appropriate awareness and operational training for administrative staff
- Proper change management disciplines and record keeping
- Annual review of risk assessments

Blue Prism is optimized to enable customers to implement Robotic Process Automation as part of a PCI compliant solution. This document references the features and functionality that are frequently utilized as part of a solution which compliment such deployments. Additional considerations also typically include: data center location and security; as well as governance and change management frameworks which are covered comprehensively within the Blue Prism Methodology.

Blue Prism Data Governance

Data Scope

The Blue Prism Delivery Methodology provides clear structure and guidance to Process Modellers at design time, encouraging them to think carefully about what data is being collected/inspected; whether it is necessary to view that data, and how the nature of that data will affect its downstream management. Clear documentation is typically generated in order to capture such design time considerations and decisions.

From a software perspective, Blue Prism provides full visibility of all data being used by a process, both from a high level input/output perspective and also as part of the in-process detail. This maximises the opportunity to provide oversight and audit of what data is being used, why it is being used and how that data is being handled.

Data Sensitivity

The PCI DSS standards stipulate that certain information may only be stored under certain conditions, while other data, such as the security code on the reverse of a card, may not be stored at all.

Sensitive data such as the card Primary Account Number (PAN) can be handled appropriately using a variety of software options:

- **Data Masking** – Where it is necessary store the full value of a particular data item (such as a password or record number), when presenting the data on screen, data masking can be used to hide all or part of the value. Likewise the data can be hashed as it is retrieved from a source system prior to being stored. E.g. Password = ********; Record Number = xx-xxxxx-879.
- **Flexible-Logging** – Granular logging controls provide flexibility to apply an appropriate level of logging based on the type of process and the sensitivity of the data being managed. For processes which include processing of sensitive data, data logging could be turned-off, or alternatively set to record the decisions and actions taken but without storing any of the data. Additionally any Blue Prism data items which are set to be of type password are automatically omitted from the logs.
- **Data Encryption** – Specific data items identified as sensitive can be encrypted prior to being stored for later processing, likewise entire work queues can be encrypted prior to storage. Where such data is stored within a work queue item, the value entered as the item key is often presented in plain-text therefore it is recommended that the key does not contain sensitive information unless it is sufficiently masked.
- **Total Encryption** – Disk level encryption of the Blue Prism database and log files can be implemented using Transparent Data Encryption (TDE) on the SQL Server database.

Data Management

The data captured and treated by Blue Prism in work queues and log files can be comprehensively managed using the data archiving feature which allows the selective archiving of data according to its age and the process it relates to.

The model governance framework that surrounds a typical Blue Prism software deployment also addresses the considerations necessary to achieve the responsible downstream storage/management/disposal of that data in a secure, managed and compliant manner.

Data Security and System Access

All data – whether operational or configuration related – is stored in a centralised and secure repository provided by Microsoft SQL Server. This makes the data easy to secure and govern which is one of the core architectural principles which underpin the Blue Prism technology platform and governance.

Secure user access control to the Blue Prism platform is provided natively or via integration with Active Directory Domain Services and is implemented using role-based permissions which govern access to system features and data at a highly granular level. Administrators apply detailed control over the actions and visibility that operational employees can achieve based on their role and permissions, while user credentials are subject to password complexity (such as length, inclusion of non-standard characters, upper/lower case etc.) and expiry rules, as well as re-use frequency restrictions.

Further Information

Please refer to the companion document entitled *Data Sheet - Operational Audit Overview* for additional information in relation to user access control, audit, and software features that provide governance of data management and security.

The guides listed below provide further insight into some of the features and functionality discussed within this document:

- *Data Sheet – Operational Audit Overview*
- *Data Sheet – Credential Manager*
- *Data Sheet – Active Directory Integration*