Rocket

COMPLIANCE

Basel III Compliance with Rocket Aldon Lifecycle Manager

Basel III is a set of international standards that focuses on the financial strength and stability of financial institutions. Though targeted at financial risks, Basel III also establishes several principles for internal controls intended to reduce the likelihood of fraud, misappropriation, errors, or misstatements that may involve technology systems. No specific, prescriptive control requirements are given, so institutions must determine the exact structure of their controls designed to satisfy the Basel III principles. From a technology perspective, Basel III is most concerned with the availability and integrity of financial data.

Where Rocket® Aldon Lifecycle Manager is involved in the development of systems that a financial institution relies on for financial reporting and stability, certain Basel III principles are relevant. Aldon Lifecycle Manager (LMi and LMe) has robust security controls available to enable a company to design and implement controls to satisfy Basel III relevant internal controls principles. The relevant requirements and capabilities that LM offers to meet them are listed on the following page.

BASEL III PRINCIPLES	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
Principle 6: An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring.	Detailed, customizable role-based access levels let an organization define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties. Developers can be restricted from making changes to software in testing or production. The ability to migrate between development, test, and production environments can also be restricted to appropriately segregated users. Reports are available showing all users with their associated access capabilities. The Community Manager module supports automated, system-driven workflows that may include access rights management and review processes.
Principle 7: An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.	All actions performed within the system, including accessing or modifying data, are logged and auditable. Reports are available showing all administrative activity performed within the system, including the modification of user access and roles.
Principle 8: An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency	ALM and its associated modules (ALM-I, ALM-Enterprise, Community Manager, and Security Service Manager) support unique user IDs for all individuals accessing the systems. Passwords are required for users to access each system. LMI also supports integration with iSeries user credentials, and Community Manager supports LDAP integration with Active Directory credentials. Detailed, customizable role-based access levels allow an organization to define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties. All actions performed within the system, including accessing or modifying data, is logged and auditable. Reports are available showing all users with their associated access capabilities. Reports are available showing all administrative activity performed within the system, including the modification of user access and roles.

Rocket

- rocketsoftware.com
- info@rocketsoftware.com
- US: 1 877 577 4323
  EMEA: 0800 520 0439
  APAC: 1800 823 405
- twitter.com/rocket
- www.linkedin.com/company/rocket-software
- www.facebook.com/RocketSoftwareInc
- blog.rocketsoftware.com