

Risk Category	Questions
Data	Are communications of confidential information over untrusted networks (i.e. Internet, leased lines) encrypted?
Data	Are passwords, PINs, and encryption keys encrypted during transmission and storage at all times?
Data	If production data is used in test environments, is all non-public customer and employee non-public information removed? If removal is not possible, is all non-public information encrypted, obfuscated, truncated, or mapped to disassociate the information from the individual to which it pertains?
Server	Are servers monitored per corporate standard?
Database	Are databases monitored per corporate standard, including administration, critical events, and sensitive transactions?
Access Management	If the application contains confidential information, is access limited to only those with a business need to know? Are roles defined to administer appropriate access?
Access Management	Are unique credentials assigned to individuals? Do credentials comply with the corporate standard for password complexity, change frequency, failed attempts, etc.? Are credentials provisioned in a secure manner?
Application	Are the business and technical owners identified?
Application	Are sensitive transactions identified and logged? Is the process to review and resolve issues defined? Are logs maintained per policy?
Application	Is developer access limited as appropriate?
Access Management	Does the application have appropriate contacts identified to assign and certify appropriate user access on a sustained basis?
Access Management	Does the solution utilize the standard approach to provision and remove users? If a custom directory is used, verify repeatable processes to ensure timely and appropriate access.
Application	Does the solution utilize standard change control processes?
Application	Does the solution utilize standard source code management?
Application	If developed internally, what are the security application development requirements? Has the team been trained in Secure Development? Have data flows been written and a threat model conducted? What role should secure dev experts play in the solution during design, test, deployment, and maintenance?
Continuity	Does the solution utilize standard backup and recovery processes?
Compliance	Identify data retention requirements and verify solution acceptance.
Compliance	If the solution supports financial systems e.g. SOx in scope, does the design support transaction integrity and completeness?
Compliance	Identify privacy, financial, and other compliance requirements. How does the design support regulatory compliance throughout design and operations? Does a point of contact exist who is accountable for regulatory compliance requirements?
Service Mngt.	What SLA's does the solution include? Should security SLA's be defined e.g. assessment frequency, post-production bugs, uptime.
Vendor	Has the vendor completed a security review? What unique contract requirements are needed? Who is the internal point of contact for vendor security requirements and issue resolution? Has legal been involved in vendor contracting?

	What compliance requirements apply to the vendor solution? How will these requirements be met, verified, and audited?
Vendor	What metrics are required to maintain visibility in vendor operational or development performance?
Continuity	Does the solution utilize standard business continuity solutions? Has a business impact analysis been performed? Who is the point of contact for BCP requirements?
Database	Is the database solution a corporate standard or new to the organization? Should a database security review be performed?
Server	Are in scope servers part of a corporate standard? Should a server configuration review be performed?
Vendor	Does the vendor have defined processes to identify, notify, and respond in the event of a security incident?
Physical	What physical security requirements should the solution include?