Grant Thornton
An instinct for growth™

Information Security

Project Security Management

Security at the core of projects

January 2018

3494GT-01-18

Security by design and by default

The designs of most new systems include security and privacy considerations. Most technology architects are sufficiently aware of the fundamentals of security, and as such there will be some protection built into the systems and software they design, hence into the project's end product.

In most cases, though, this is not enough – usually through no fault of the designers or implementers. Security is a large, complex and fast-moving subject area, and as such many projects require specialist advice and input in order to implement effective security in what they deliver.

After go-live

Putting a system live is not the end of the project: go-live should not take place unless a solid, well-defined operational regime of patching and security review is in place for at least the first 12 months of operation.

The Project Security Manager

Many organisations would not think twice about engaging a third party project manager (PM) to drive their key projects: external PMs provide expertise and experience that may not exist within the organisation, and provide additional resource in time-poor organisations. The same logic applies to a project security manager, who brings insight and control to a project to ensure it complies not just with the stated requirements but also with the organisation's security policies and industry best practice.

Evolving best practice

Industry best practice evolves, and you must keep up with it. For example modern laws require data protection to be core to the design and implementation of systems. A PSM will help you ensure your design and implementation align with best practice.

What Grant Thornton can do for you

As a project security manager our consultant will:

- Ensure that all security requirements are detailed as part of the specification phase.
- Work with designers and architects to ensure that the security requirements are addressed in the most effective way.
- Participate in change control processes to ensure security requirements are dealt with.
- Oversee the security aspects of development and implementation.
- Assist with the construction of test plans.
- Advise test staff and assist with remediation.
- Design the post-go-live security regime under which the product or system will operate.
- Assess security readiness prior to go-live.
- Carry out a post-go-live assessment to ensure the security elements are being operated correctly.

For more information please contact:

David Cartwright
Senior Consultant, Information Security
T +44 (0) 1534 885813
E david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

grantthorntonci.com