CESG

Technology and Information Risk

Decision making do's and don'ts

Make sure that you	Ensure that you don't
...understand what the organisation is about and what it is trying to achieve to provide context for risk assessment and risk management decisions.	...conduct risk assessment and make risk management decisions in isolation and without understanding the business context.
...conduct risk assessment and manage risks for the whole development, design, implementation and in-service lifecycle of a system or service.	... retrofit risk assessment and management onto solutions where security relevant design decisions have already been made. Don't assume that once a service or system is in service that there is no need to continue to manage risks.
...understand what it is about your organisation's assets and services that the business cares about. Consider what else is important to the organisation (ie reputation, service reliability, customer privacy, customer wellbeing and safety).	...just think about the confidentiality, integrity and availability of information assets.
...use people who have the necessary technical, security and business skills to objectively assess risks and communicate them to the organisation.	...employ resource to use risk assessment methods and tools to generate unusable lists of risks that do not take account of the needs of the organisation.
...conduct risk assessment to inform information security risk management decisions.	...conduct a risk assessment simply to satisfy a project milestone.
...scale your risk assessment activities as necessary to support different risk management decisions across the organisation.	...assume you can use the same approach to identify, analyse and evaluate risk across the whole organisation. One size does not fit all.
...communicate risk assessment inputs and outputs in a meaningful way.	...input meaningless words or numbers into forms, spreadsheets or tools. Don't generate meaningless outputs from methods or tools, and expect them to be understood and consistent.
...communicate risks at the appropriate level of detail required by the audience, translating into meaningful language where required.	...assume that everyone who needs to will understand your risks. Don't use security jargon when describing risks to decision makers, and don't use business language for suppliers and developers if they need to understand the technical details.
...reuse risk assessment information that is available for common solutions.	...redo risk assessments if there is no difference between the common solution and what the organisation is doing.
...create baselines for risk assessment inputs (eg threat) based on the best information available, and use them until something significant changes.	...rely on risk analysts and practitioners to make isolated decisions on risk assessment parameters whilst expecting the output to be consistent.
...prioritise the output of risk assessments based on what is important to the organisation and the considered impact on it.	...rely on arbitrarily chosen risk appetite, tolerance or level boundaries and a check list of controls to govern what risk management actions are taken.
...incorporate and apply real security measures into technology solutions as a result of good risk assessment and risk management decisions from the outset.	...expect that simply following a risk management process will deliver real security without proactive, engaged and intelligent risk management action and decision making throughout.
...ensure that security requirements in contracts and service level agreements are informed by and traceable to real risks.	...simply say in contracts and service level agreements that systems or services should be accreditable or compliant with a particular standard.
...document risk assessments and key risk management decisions for traceability and accountability purposes.	...create large and unnecessary document sets and unmanageable or unusable lists of risks.