Risk assessment checklist - Plan and organize

Check "Yes" or "No" or "N/A" (where not applicable). Where a No is indicated, some action may be required to rectify the situation. Cross-references (e.g., See FN 1.01) point to the relevant policy in the First Reference Internal Control Library. **FN** = Finance & Accounting PolicyPro, Volume 1; **GV** = Finance & Accounting PolicyPro, Volume 2; **OP** = OMPP policies in FAPP electronic version; **IT** = Information Technology PolicyPro; **NP** = Not-for-Profit PolicyPro.

Clear entire form

Plan and Organize risks to consider		Yes	No	N/A	Comments / Action Required
Define a strategic IT plan and direction					
PO1	Do you have a policy requiring that IT strategic and tactical plans be prepared and maintained? See IT1.01, 1.02, 12.01	☐	☐	☐	
PO2	Do you ensure that strategic plans lead to tactical plans? See IT1.01, 1.02	☐	☐	☐	
PO3	Do you mandate that IT planning happens at least once a year? See IT IT1.01, 1.02	☐	☐	☐	
PO4	Have you developed or acquired a standard planning approach and methodology? See IT1.01, 1.02	☐	☐	☐	
PO5	Is the IT strategic plan related to your organization's objectives and business plans? Does it evolve as those plans are updated? See IT1.01	☐	☐	☐	
PO6	Does your strategic plan correspond with your risk appetite? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	
PO7	Are objectives and plans reassessed as frequently as required, commensurate with the rate of change in technology, threats, risks and business opportunities? See IT1.01, 1.02	☐	☐	☐	
PO8	Do managers of other business units participate in the IT strategic planning exercise? See IT1.01	☐	☐	☐	
PO9	Have you established committees or regular meetings between business and IT management to share information and promote synergy? See IT1.01	☐	☐	☐	
PO10	Do you have a process where appropriate business and IT executives approve the strategic and tactical plans? See IT1.01, 1.02	☐	☐	☐	
PO11	Does the planning process consider technology trends and developments, and relevant architecture elements? See IT1.01, 1.02	☐	☐	☐	

© 2008-2010 First Reference Inc. All Rights Reserved.

Risk assessment checklist - Plan and organize

Plan and Organize risks to consider		Yes	No	N/A	Comments / Action Required
PO12	Do you obtain input to the planning process from key stakeholders, including employees, customers, and suppliers? See IT1.01, 1.02	☐	☐	☐	
PO13	Have you developed a communication strategy to maximize the exposure and acceptance of the IT plans throughout the organization?. See IT1.01, 1.02	☐	☐	☐	
PO14	Have you assigned responsibilities for the development, approval, communication and monitoring of IT objectives and plans? See IT1.01, 1.02	☐	☐	☐	
PO15	Do you mandate that senior management must consider IT plans when making decisions related to technology within their business units? See IT1.01, 1.02	☐	☐	☐	
PO16	Do you obtain feedback about the quality and usefulness of IT plans from senior management across the organization, and from the staff who use the plans? See IT1.01, 1.02	☐	☐	☐	
PO17	Have you considered forming a high-level IT security steering committee including senior IT managers and business process owners to assess risks and identify gaps? See IT 1.02, 1.03	☐	☐	☐	
Define IT processes, organization and relationships					
PO18	Is IT an active participant in establishing the organization's overall objectives and business strategies? See IT1.01	☐	☐	☐	
PO19	Is there a process for establishing an owner for each IT component? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	
PO20	Are the roles and responsibilities for each category of owner established and communicated across the organization? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	
PO21	Are ongoing periodic reviews performed to confirm that established responsibilities and accountabilities remain relevant and are being met? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	

© 2008-2010 First Reference Inc. All Rights Reserved.

Risk assessment checklist - Plan and organize

Plan and Organize risks to consider		Yes	No	N/A	Comments / Action Required
PO22	Do you assign responsibilities so that no single individual has authority to add, modify or delete an information asset without there being an independent review of that activity? See IT1.03, 4.02	☐	☐	☐	
PO23	Do you maintain separation of duties between initiation and authorization activities? See IT1.03, 4.02.	☐	☐	☐	
PO24	Do you maintain separation of duties between implementation (or execution), and verification activities? See IT1.03, 4.02	☐	☐	☐	
PO25	In processes with a high degree of risk, are key business functions separated, so that no individual can add, modify or delete information or transactions? See IT1.03, 4.02	☐	☐	☐	
PO26	Do you have policies to maintain separation of duties during vacations, illnesses or leaves of absence? IT1.03, 4.02	☐	☐	☐	
PO27	Have you created data management policies that assigns responsibilities for data management activities to appropriate information resource owners and users? See IT5.04	☐	☐	☐	
PO28	Do you have policies that ensure that the custodians and users of data maintain the confidentiality of the data according to the classification assigned by data owners? See IT9.02	☐	☐	☐	
Manage IT human resources					
PO29	Are departmental and individual performance plans linked to and integrated with IT technology objectives and plans? See IT1.01, 1.02	☐	☐	☐	
PO30	Are recognition and reward mechanisms related to the achievement of IT objectives and plans? See IT1.01, 1.02	☐	☐	☐	
PO31	Do you have a IT skills inventory and compare it to the required skills periodically to identify potential gaps? See IT12.01	☐	☐	☐	
PO32	Do you have a process or plan to eliminate skill gaps through training, supervision, acquisition, contracting, hiring or outsourcing? See IT12.01	☐	☐	☐	

© 2008-2010 First Reference Inc. All Rights Reserved.

Risk assessment checklist - Plan and organize

Plan and Organize risks to consider		Yes	No	N/A	Comments / Action Required
PO33	Do you maintain IT succession plans to ensure that the necessary skills and experience will be available in the future? See IT 12.01	☐	☐	☐	
PO34	Have you created accountability for organizational security in position descriptions and performance objectives? See 12.01, 12.02	☐	☐	☐	
PO35	Do you have a process to communicate HR changes (e.g., terminations, transfers) to the individuals responsible for maintaining security privileges?	☐	☐	☐	
Manage quality					
PO36	Have you established policies and standards to ensure the efficiency and effectiveness of the systems development and acquisition process? See IT2.02, 3.02	☐	☐	☐	
PO37	Have you defined the role of financial and internal audit representatives and the extent of their involvement in systems development and acquisition? See IT2.02, 3.02, 7.03	☐	☐	☐	
PO38	Have you established procedures to ensure that application code is consistent with design specifications and meets the organization's standards for programming languages, documentation, code structure, naming conventions and processing controls? See IT2.02, 3.02, 4.01	☐	☐	☐	
PO39	Have you created and communicated standards for programming languages, documentation, code structure, naming conventions and processing controls? See IT2.02, 3.02	☐	☐	☐	
PO40	Do you confirm the quality of the code using supervisor review, unit testing and independent quality assurance reviews? See IT2.02, 3.02	☐	☐	☐	
PO41	Have you created a quality assurance function to independently test code for functionality, and to review the code and accompanying documentation for compliance with standards and maintainability? See IT2.02, 3.02	☐	☐	☐	

© 2008-2010 First Reference Inc. All Rights Reserved.

Risk assessment checklist - Plan and organize

Plan and Organize risks to consider		Yes	No	N/A	Comments / Action Required
Assess and manage IT risks					
PO42	Is the importance of IT risk captured in organization-wide policies, standards and procedures and effectively communicated to all personnel at all levels? See IT1.05, 1.06	☐	☐	☐	
PO43	Do management decisions and conduct reflect risk management and control principles? Is this communicated to employees and in corporate communications to outside stakeholders? See IT1.05, 1.06	☐	☐	☐	
PO44	Is risk management included in performance evaluations of business units, technology support areas, and systems? See IT1.05, 1.06	☐	☐	☐	
PO45	Is there an ongoing employee awareness program to enforce the organization's risk culture? See IT1.05, 1.06	☐	☐	☐	
PO46	Is the organization's risk assessment process a key reference when preparing information for IT strategic and tactical plans? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	
PO47	Have you established procedures to survey the internal and external environment to identify changes in business or technology risks? See IT1.01, 1.02, 1.05, 1.06	☐	☐	☐	
PO48	Are there clearly defined responsibilities and accountabilities for IT risk management? See IT1.05, 1.06	☐	☐	☐	
PO49	Have you established a steering committee for IT risk management and control to direct risk management programs and monitor their effectiveness? See IT1.05, 1.06	☐	☐	☐	
PO50	Do position descriptions include responsibilities and accountabilities for risk management? See IT1.05, 1.06	☐	☐	☐	
PO51	Do management objectives include targets and indicators for risk management? See IT1.05, 1.06	☐	☐	☐	
PO52	Does responsibility for risk management ultimately lie with the owners of the components? See IT1.05, 1.06	☐	☐	☐	

© 2008-2010 First Reference Inc. All Rights Reserved.