7.1 The Company

The hypothetical company is a publicly traded manufacturer and supplier of commodity products used as feeder stock by consumer product manufacturers in different markets around the world. The company's profile is as follow:

- US $7 billion in total assets.
- Based in the United States.
- Thirty production facilities in seven countries, including Belgium, China, Qatar, Saudi Arabia, Singapore, South Korea, and the United States.
- Six research, technology, and quality control centers located in each production facility.
- Five thousand employees worldwide.
- Five major competitors.
- Holds nearly 3,000 domestic and international patents and patent applications.
- Three major business units for manufacturing operations along product lines, centralized headquarters, and support-service organizations.
- Three major capital projects to build and expand manufacturing capacity.

In addition, the company's centralized IT organization consists of four basic divisions:

- Global infrastructure:
  - Telecommunications.
  - Voice communications.
  - Networks.
  - Remote connectivity.
  - Desktop and Internet.
  - Information life cycle management.
  - Servers.

- Enterprise applications:
  - One major ERP application used throughout the company for supply chain management, financial accounting, human resources (based in the United States), sales, and distribution.
  - Also supplies SAP technical support and Advanced Business Application Programming (ABAP).

- Manufacturing Systems:
  - Responsible for systems operating at manufacturing facilities.
  - Local applications include payroll for non-U.S. sites, research and quality control databases, environmental reporting, and manufacturing process control systems.
  - Financial analysis and controls.

- Strategy and risk management:
  - Contracts, purchasing, and licensing.
  - Strategy, architecture, and standards.
  - Security services.
  - IT change and governance.
  - Project management office.

The manufacturing facilities are the organization's lifeblood. Because they are located throughout the world and have different capacity sizes, they introduce risks that may impact business fundamentals and financials. Furthermore, although the manufacturing facilities create a somewhat decentralized business model, the organization's centralized corporate and service elements offer the opportunity for process-based audits that cross business functions.

In the area of compliance, the organization is subject to U.S. and European requirements, including Sarbanes-Oxley, the European Union's Directive on Data Protection (Privacy), the U.S. Foreign Corrupt Practices Act, and other similar regulations in the locations in which it operates. According to the annual business plan, several major capital investment projects are under way that will have a great impact on the organization's future competitiveness.

Finally, the company's IT function aligns closely with its business model. The company uses a fairly homogeneous group of applications, including a standard ERP application, a global network and server infrastructure, and standard support processes for IT service delivery functions, governance, and security.

7.2 The IT Audit Plan

Based on this description, an IT audit universe can be identified that defines a holistic inventory of conceivable audit subject areas and provides management with information on the effectiveness of their control environment and operations.

As mentioned in the previous paragraphs, the centralized corporate and services elements offer the opportunity for global, process-type audit subjects. The company's centralized ERP application, global infrastructure support areas, and standard IT service delivery processes are good candidates for independent audit subjects covering large areas of IT risk.

Manufacturing facilities also are represented in the IT audit universe with subjects from locally supported applications

and an underlying infrastructure (shown as facility 1–30 for simplicity in table 7). These audit subjects are likely to be aligned with business process audits in each facility.

Table 7 shows what a sample universe of potential IT audit subjects might look like for the company. Each of the 30 manufacturing facilities has these and other audit subject areas.

Business Unit	Audit Subject
Corporate	Network administration and security
Corporate	Remote connectivity
Corporate	Windows Server administration and security
Corporate	UNIX administration and security
Corporate	ERP application and general controls
Corporate	Sarbanes-Oxley sustainability review
Corporate	Corporate privacy compliance
Corporate	Database administration and security
Corporate	IT governance practices
Corporate	ITIL deployment practices
Corporate	Application program change control
Business Segment 1–3	Major capital investment projects (e.g., information protection and corporate compliance)
Facility 1–30	IT infrastructure
Facility 1–30	Human resources and payroll application
Facility 1–30	Process control systems

Table 7. IT audit universe

After the IT audit universe is defined at a high level, the next step is to assess the business and IT risks on each area. Risk categories are assessed based on their likelihood of occurrence and the impact they would have on the organization if the risk was not adequately managed. This risk approach uses relative ranking as shown in table 8. For example, a three-point scale to assess likelihood and impact is used as outlined in the following description:

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Impact Scale (Financial)		
H	3	There is a potential for material impact on the organization's earnings, assets, reputation, or stakeholders.
M	2	The potential impact may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

Table 8. Three-point likelihood and impact scale

To aid in the analysis, a range is selected that indicates a relative risk ranking of high, medium, and low, as follows:

Level	Composite Risk Score Range	Recommended Annual Cycle
H	35–54	Every 1 to 2 years
M	20–34	Every 2 to 3 years
L	6–19	Every 3 to 5 years

Table 9. Range of relative risk ranking

As part of the risk assessment step, auditors need to define a recommended annual cycle for audit subjects in the universe based on composite risk score ranges, where high-risk audit subjects are reviewed every one to two years, medium-risk subjects every two to three years, and low-risk subjects every three to five years. This will ensure that high-risk areas are reviewed frequently and low-risk areas are covered adequately over a five-year span. Table 10 on page 24 shows an example of a completed risk assessment.

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	3	2	3	2	2	1	41	H
Facility 3 – HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
Facility 3 – IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Facility 3 – Process Control Systems	3	3	3	2	3	3	3	3	2	2	2	1	39	H
UNIX Administration and Security	2	2	3	2	3	3	2	3	3	2	2	2	35	M/H
Corp. Privacy Compliance	3	1	3	3	3	3	2	1	2	1	3	3	34	M/H
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Facility 1 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Facility 1 – Process Control Systems	2	3	3	2	2	2	3	3	1	1	1	1	27	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
Facility 2 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Major Capital Investment Projects	2	2	3	3	1	1	2	2	1	1	2	3	25	M
Application Program Change Control	2	3	2	3	1	2	2	2	1	3	1	2	23	M
SOX Sustainability Review	2	2	2	3	2	2	1	2	2	2	1	2	22	M
Network Administration and Security	2	2	2	1	2	2	2	2	2	2	2	2	22	M
Facility 2 – Process Control Systems	2	2	2	2	1	2	2	2	2	2	1	1	19	M/L
ITIL Deployment Practices	1	2	2	3	3	1	3	1	1	3	2	1	19	M/L
Facility 2 – HR/Payroll Application	1	2	1	2	2	3	2	2	3	1	1	2	19	M/L
Facility 30 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 1 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 30 – IT Infrastructure	1	1	3	1	1	1	2	2	2	1	1	1	12	L
Facility 30 – Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L

L = Likelihood
I = Impact

Table 10. Risk assessment

Once risk assessment results are available, the next step is to formalize the audit plan. As discussed in section 6, the audit plan consists of risk-driven audit projects, mandatory compliance reviews, stakeholder requests, and follow-up audits of previously identified significant issues. Because these tasks need to be completed using available internal audit resources, some risk-driven audit projects might not be incorporated in the plan.

Continuing with the hypothetical company example, the board has asked the IT department to be involved in the coordination of an external infrastructure penetration test, and operating management has requested assurance that Sarbanes-Oxley management testing is sustained throughout the organization. In addition, the IT function asked the internal audit department to be involved with an ITIL deployment project to identify whether service delivery processes are effective and cover all risks.

These stakeholder requests are accepted because they fit with the mission of the internal audit department and will be added automatically to the audit plan. Furthermore, there was a significant segregation of duties issue identified in the previous year's procurement process audit, so a follow-up review will be added to the plan to ensure agreed upon remediation efforts are progressing as planned. In the compliance area, compliance with the new corporate policy on protecting personal data for privacy will be included because there are plans to transmit personal data between non-U.S. facilities and the U.S. corporate headquarters.

The company has an IT audit staff of five auditors or approximately 1,000 available days for engagements after considering exception time and training. Based on the risk assessment of available audit subjects, mandatory activities, and stakeholder requests, the most effective audit plan is shown in table 11.