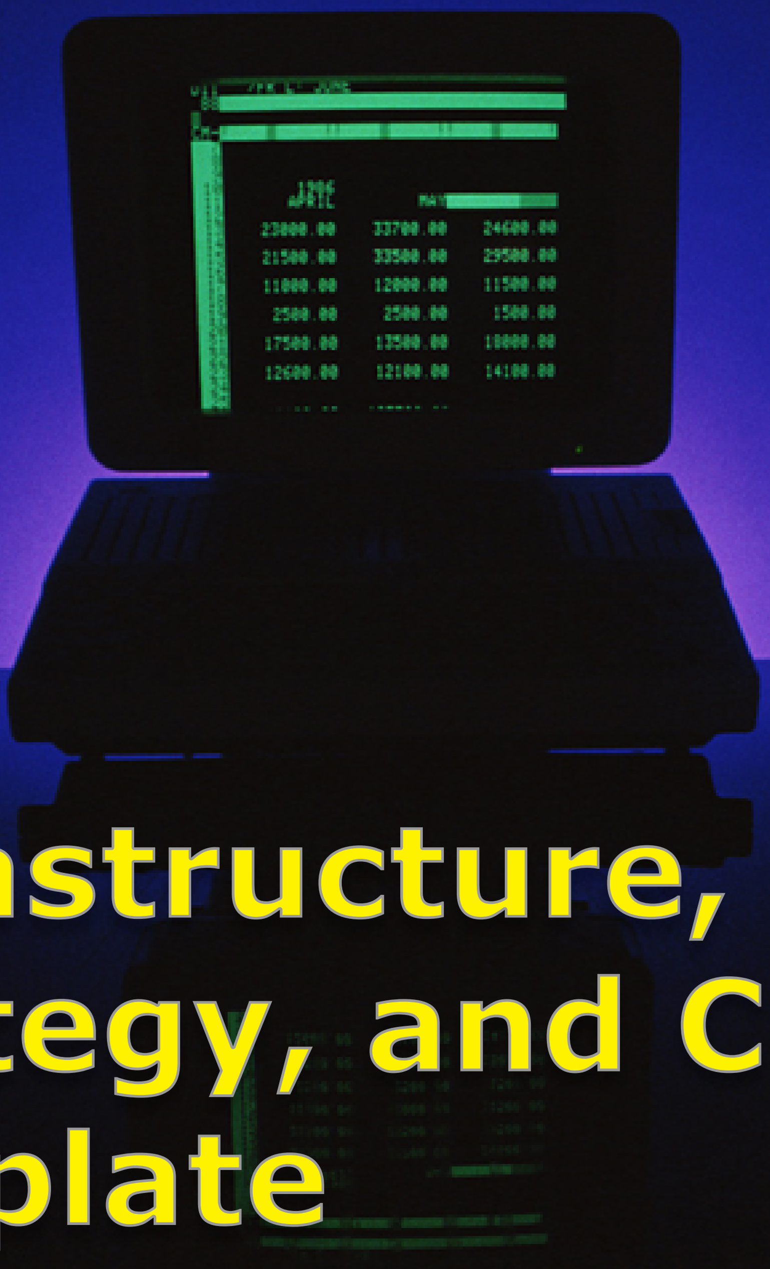
Information Technology



Infrastructure, Strategy, and Charter Template

ISO 2700, GDPR, HIPAA, PCI-DSS, and CoBit Compliant

Janco Associates, Inc.

Version 3.6

Table of Contents

IT Infrastructure, Strategy, and Charter Summary

[Enterprise] Information Technology (IT) is a large and diverse organization that manages the information, internet, communication, and computer resources of [Enterprise]. This document

- Defines IT responsibilities that are the building blocks of a well-performing organization
- Highlights the overall guidelines and policies of [Enterprise] IT
- Provides an understanding of how IT integrates with the enterprise
- References additional documentation that addresses more tactical standards and guidelines found throughout the company

Benefits of IT Infrastructure Management

IT Infrastructure management commonly supports operational functions such as system management, change control, release management, network management, applications management, job management, and database management. Across these functions, IT Infrastructure management provides a number of benefits that can result in cost savings, improved service levels, and operational efficiencies. Benefits include:

- edures, and
  ture alerts and
  dardization can
  tions and by
  aff member. For
  individual system

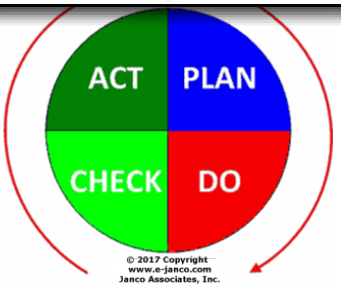
- **Leveraging of staff resources, leading to increased IT productivity** - Productivity is a measure of how much staff time can be spent on work that brings value to the business - such as deploying new or improved applications to increase competitive advantage. Use of a standardized infrastructure management processes can help increase the proportion of staff time that can be used for more productive work that can increase business value in addition to improving the service levels provided by IT.
- **Higher availability and improved IT Service Management** - With enterprise operations throughout the organization increasingly depending on information systems, system and network availability are key IT and enterprise requirements. While costs vary based on factors such as the nature of the applications, any unplanned downtimes have direct costs that arise from loss of business opportunity and decreased end-user productivity. The use of infrastructure management processes can reduce downtime, improve application performance, and improve revenue opportunity to the business.
- **Faster response to incidents** - The use of standardized infrastructure management processes can greatly improve the speed with which IT can respond to service disruption incidents. This can occur in a number of ways, including standardized responses to simple alerts and alarms; creation of trouble and repair tickets for service desk functions; and problem determination and resolution aids such as event correlation, impact analysis, and root cause analysis.

- Forming the foundation and mechanism for informed decision making
- Enhancing corporate governance and compliance-related activities
- Increasing efficiencies and consistency – bringing order to centralized or distributed environments

- **ISO 27002** – The ISO 27002 standard is a renaming of the ISO 17799 standard, which is a code of practice for information security. It outlines controls and control mechanisms, which may be implemented subject to the guidance provided within ISO 27001.

  The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

- I etely defined.
  T uidance for the
  i m). The
  p e in
  i released. ISO
  2 hen
  e



- **ISO 27004** - This is the designated number for a PROPOSED standard covering information security, system management, measurement, and metrics.
- **ISO 27005** – This is the name of a PROPOSED standard emerging standard covering information security risk management. As with the other standards within the ISO 27000 series, no firm dates have been established for its release. However, it will define the ISMS risk management process, including identification of assets, threats, and vulnerabilities. This is the ISO number assigned for an emerging standard for information security risk management.
- **ISO 27006** - This standard offers guidelines for the accreditation of organizations that offer certification and registration with respect to ISMS.

Strategy and Charter Statement of Authority

The strategy and charter statement of authority for IT includes all information technology, internet, e-commerce, and communications, which support the business goals of [Enterprise], while:

- Maintaining production performance at a level that reflects a "Service Excellence" philosophy
- Seeking out and implementing solutions that effectively satisfy business process requirements and creatively exploit business opportunities

Chief Information Officer (CIO)

Strategy and Charter

1. Guides the development of the overall Information Technology(IT) strategies and planning
2. Participates as a member of the [Enterprise] executive management team
3. Interacts frequently with senior and functional management on internal and external information related issues

or services

functional

ications
nce, SAP)

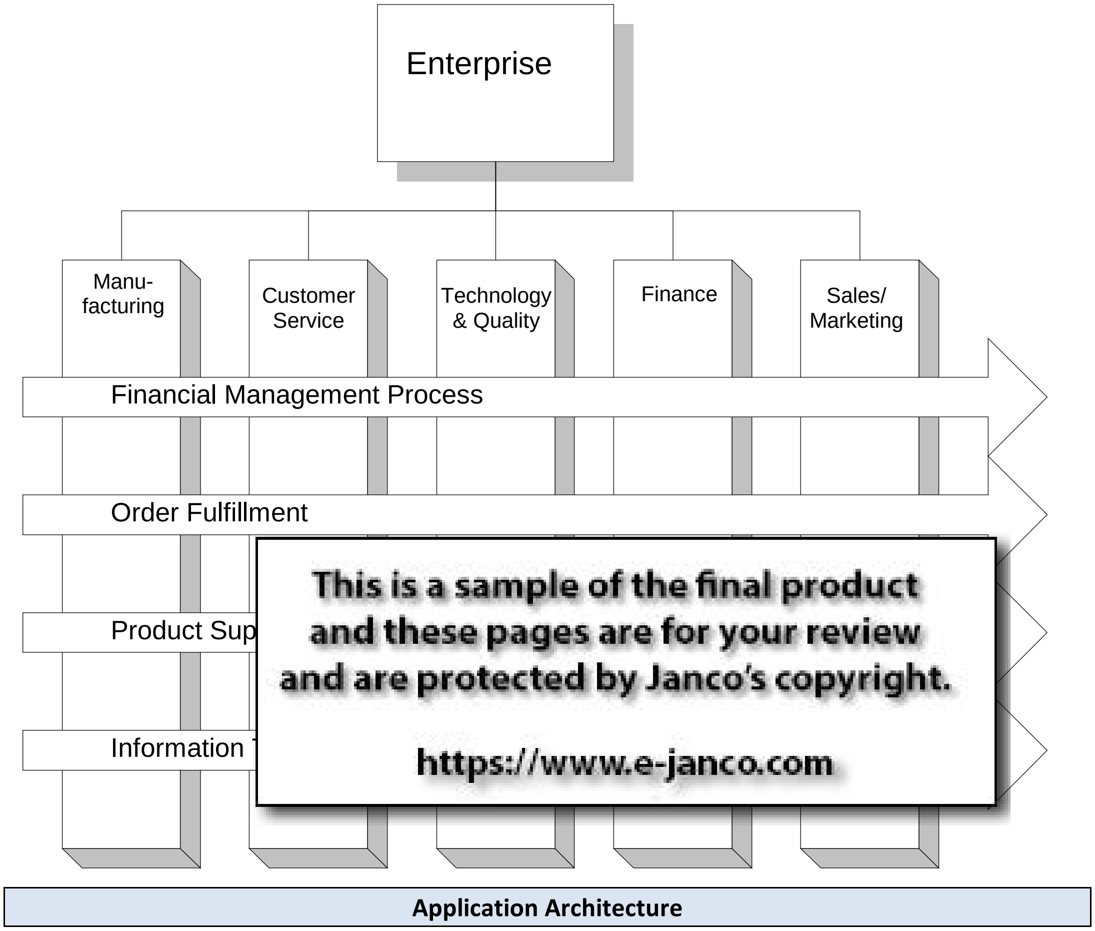
hitectural
infrastructure for [Enterprise] systems processes

8. Develops and maintains statements of necessary policies and procedures to assure proper documentation and communication of [Enterprise] IT related activities
9. Participates in the evaluation of IT functions and staff within [Enterprise]
10. Identifies opportunities and provides appropriate guidance for information systems staff career development throughout the organization.
11. Maintains external links to other companies and professional and academic organizations to gain competitive assessments and share information
12. Provides company-wide direction on the use of emerging technologies of IT within the enterprise. Identifies the information technologies to be assimilated, integrated and introduced within the corporation

IT Management Structure

Organizational Approach

The IT organization is structured around the way the various business functions operate. In addition to that, the overall future system architecture is as depicted in the graphic that follows.



IT Job Family Classification

Structure

Other [Enterprise] Resources

- ✓ [Enterprise] Human Resources Representative
- ✓ [Enterprise] Common Office Network and Work Station and PIM Orientation Manual(s)
- ✓ Training & Development Resource Guide
- ✓ IT Job Family Classification at https://www.e-janco.com/it-Job-Family.html
- ✓ IT and Internet Job Descriptions from Janco Associates at https://www.e-janco.com/Job_Book.htm

A job family classification system is one that defines how individuals can grow into higher level positions over time by providing benchmarks milestones that need to be achieved as they advance over time. This in time impacts the compensation that is paid in a fair and objective manner. A job family is a series of progressively higher, related jobs distinguished by levels of knowledge, skills, and abilities (competencies) and other factors, and providing promotional opportunities over time.

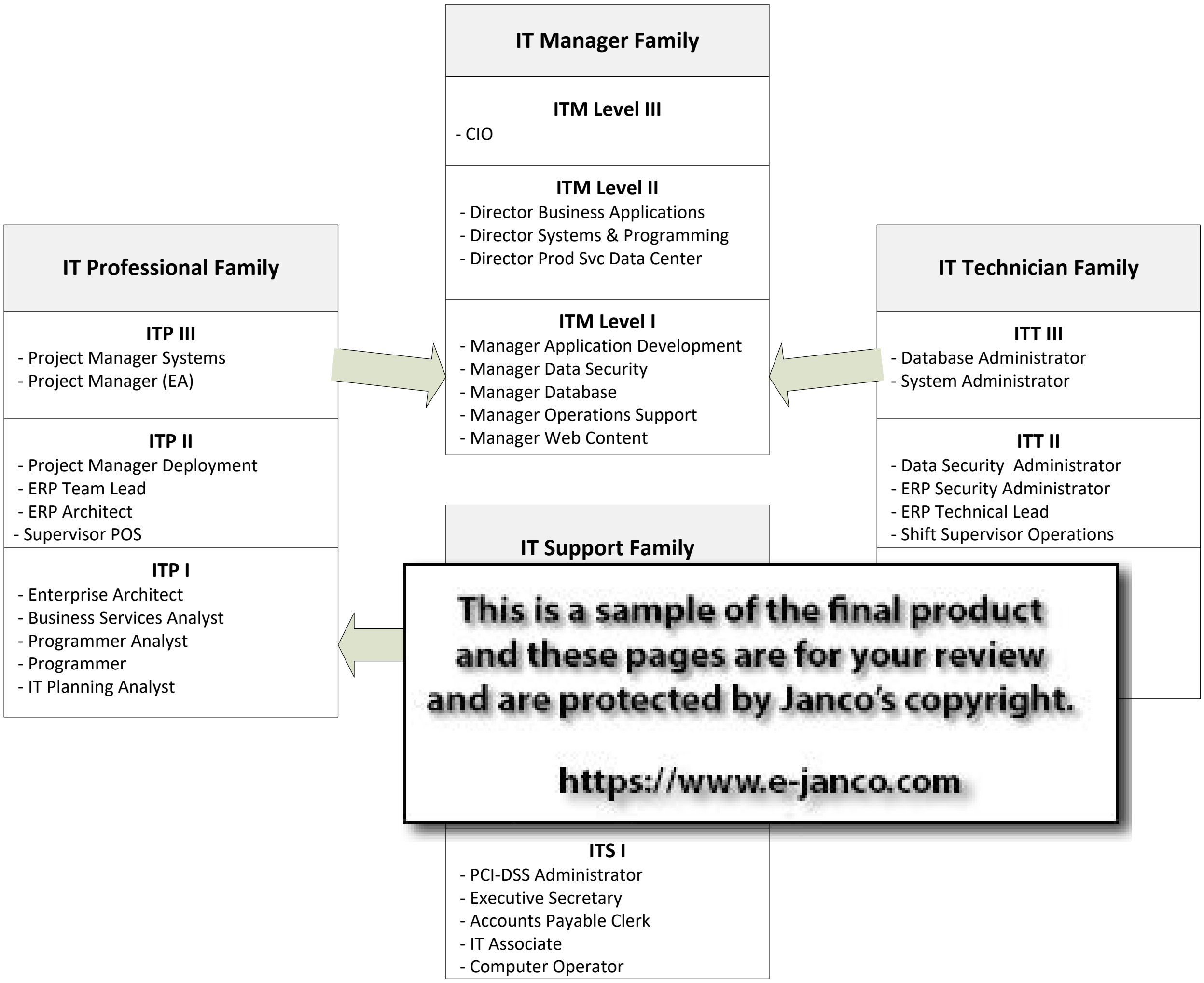
The approach that we have found that works the best has four (4) primary job, families

- **Managemen** Technology r nd scope of the information systems or s ed by the applic d responsibilit

- **IT Professional Level** - This family consists of several levels of Information Technology Professional work – working Professional through Supervisor/Expert. Levels are distinguished based on the complexity and scope of responsibilities, the degree of specialization and the degree of independent functioning. Included within this level are all of the development activities.
- **IT Technical Level** - This job family consists of levels of Information Technology Technical work distinguished by the complexity of the responsibilities assigned and characterized by the type of equipment, operating systems or subsystems supported. This job family is distinguished from the Information Technology Professional in that its main emphasis is on installing, maintaining, and troubleshooting network and information technology systems and assisting with their on-going use and operation.
- **IT Support/Entry Level** - This job family consists of five levels of Information Technology Consultant work which are distinguished by the complexity of the responsibilities assigned and characterized by the type of equipment, operating systems or subsystems, and interactions with client users. Positions allocated to this

job family differ from those in the professional or technical categories in that assignments are more administrative in nature, involving the completion and coordination of various information services requirements rather than having direct responsibility for the technical aspects of the information system.

IT Job Families



IT Manager Family

ITM Level III
- CIO

ITM Level II
- Director Business Applications
- Director Systems & Programming
- Director Prod Svc Data Center

ITM Level I
- Manager Application Development
- Manager Data Security
- Manager Database
- Manager Operations Support
- Manager Web Content

IT Professional Family

ITP III
- Project Manager Systems
- Project Manager (EA)

ITP II
- Project Manager Deployment
- ERP Team Lead
- ERP Architect
- Supervisor POS

ITP I
- Enterprise Architect
- Business Services Analyst
- Programmer Analyst
- Programmer
- IT Planning Analyst

IT Technician Family

ITT III
- Database Administrator
- System Administrator

ITT II
- Data Security Administrator
- ERP Security Administrator
- ERP Technical Lead
- Shift Supervisor Operations

IT Support Family

ITS I
- PCI-DSS Administrator
- Executive Secretary
- Accounts Payable Clerk
- IT Associate
- Computer Operator

Strategy

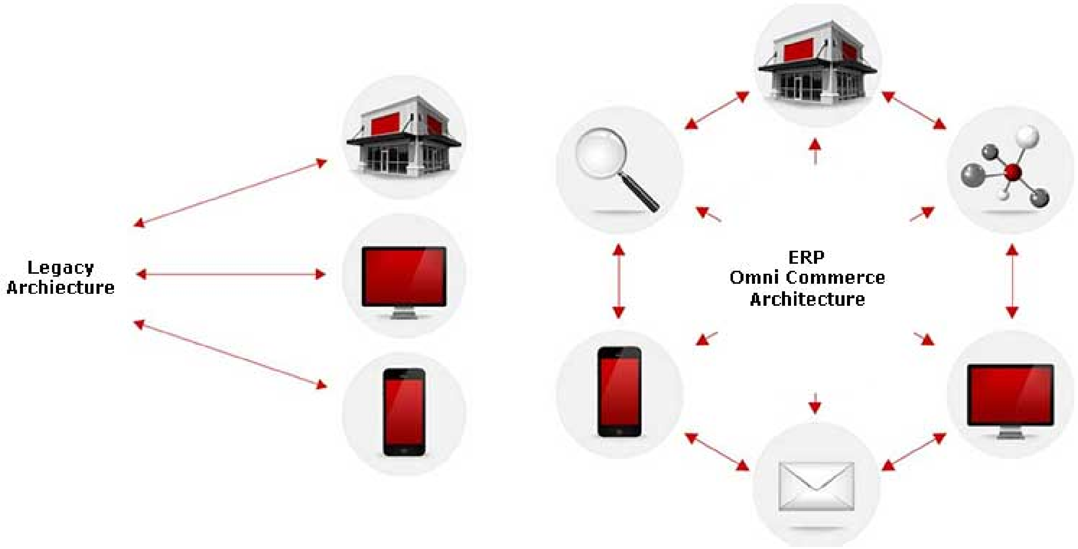
Over 80% of small to mid-sized businesses (SMB) and all large business focus on customer and supplier re-engagement and channel development programs via social media. There is extreme price and value-based competition with this arena. There is a requirement to present the outside world with more choices and interaction capabilities.

To be successful, an ERP and/or Omni commerce implementation must adhere these certain criteria need to be met:

- The driver for the effort needs to be a member of the “Operational” executive management team or the CEO
- There needs to be active support and management by a cross-functional team from operations, finance, marketing, distribution, sales and Information Technology (IT)
- Implementation success should be measured utilizing ROI principles and operational impact (productivity)
- Closely aligned with the industry and able to grow as a company changes to meet demand

Some l a move to ERP and or Omni Comm by the Internet and direct interac e of the control of the IT functio

Legacy lication is for a single purpose. The gr acy based application versus an ERP



Top 10 Best Practices for Omni Commerce Implementation

1. The Internet commerce function should be a top priority have a business "champion" who is pushing for it – not just the IT pros in the enterprise

2. Create an infrastructure strategy that addresses both traditional procedural solutions and ones that leverage cloud-based application. You do not have to invent – utilize the work of others. (See IT Infrastructure, Strategy, and Charter Template -- https://www.e-janco.com/Infrastructure.html)

   - **Authenticity:** The same fundamental set of core values around the products and/or services and what the company stands for in a brick-and-mortar context should be integrated throughout the Online presence.
   - **Consistency**: The user experience should be aligned with the overall brand, to have the same 'look and feel' between Internet platforms and brick and mortar assets.
   - **Transparency**: Communications with users at all levels must be consistent across Internet and brick-and-mortar platforms

3. Prototype the design of the overall experience to test the user-experience and minimize the cost of new development that may not produce the results you want.

petitive advantage. A perfect
vironment and meets all of the

roducts and/or services.
/ are the ones will benefit the most

7. Utilize social media sign-in to minimize password fatigue. Surveys have found that more than 75% of all shopping cart activity is abandoned at the sign-in step.

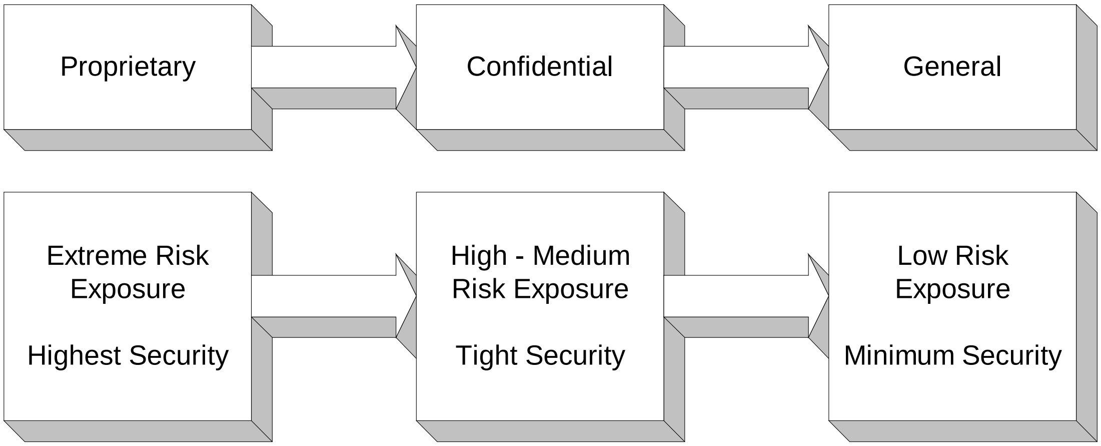
8. Design content and site flow to be device independent. The user may start on a desktop; move to a SmartPhone; and then complete the activity on a tablet.

9. Move away for "3 column" design to panel design. Design with "large" images as the focal point so that the user experience is improved.

10. Display products and services in natural settings – not as stand-alone images. This helps to provide reference points for the user looking at the product.

Classification Of Data, Software, And Documentation

All data, software, and documentation are classified based upon its criticality. Criticality is defined as the relative measure of impact on [Enterprise] by inadvertent or deliberate disclosure (i.e., loss of privacy and/or confidentiality), alteration, destruction or non-availability of that resource.



Data Classification

The classification of the data, software, or documentation determine the:

- Classification of the systems and facilities processing or storing that information; and
- Labeling, handling, and distribution of that information.

The

Appendix

CIO and CTO Expanded Roles

The CIO and CTO have had their roles expanded as more businesses have moved to an Internet-based environment from the traditional “brick and mortar”. The job description for these positions, which are included as separate attachments, have been expanded accordingly.

Responsibility	CIO and CTO Traditional Roles	CIO and CTO Value Added Role
Strategy and Planning	• Define, Update, and implement IT Strategy • Manage IT across the enterprise	• Align IT objectives and programs with enterprise objectives and strategies • Coordinate IT across the enterprise
Control	• Align IT teams with enterprise performance objectives • Control performance objectives • Control overall technology budget	• Define KP metrics based on overall enterprise objectives • Report performance status • Coordinate overall technology budgets
Service	• Acquire software/hardware • Select, manage, and control IT [illegible]	• Maximize mix of in-house versus outsourced providers [illegible]
Risk Management	[illegible]	[illegible]
Business Processes	[illegible]	[illegible]
Strategic IT Initiatives	• Plan and manage strategic IT initiatives • Manage application portfolio • Manage IT projects	• Shift decisions to enterprise operational groups • Include enterprise process executive in IT governance
Enterprise Infrastructure & Applications	• Define standards and architecture • Coordinate (consolidate) IT processes across the enterprise	• Optimize services through a mix of internal and external services • Coordinate security and compliance

Job Descriptions

The job descriptions listed below are part of the original download. They are included in a secondary directory (Job Descriptions) and not part of this document, the pdf, nor the ePub versions of it.

CIO Job Description

CIO Job Description (small enterprise)

Chief Digital Officer

Chief Mobility Officer

Chief Security Officer

Chief Technology Officer

Digital Brand Manager

What's News

Version 3.6

- Added 3 full Job descriptions
  - Chief Mobility Officer
  - Chief Security Officer
  - Chief Technology Officer
- Updated all of the included job descriptions
- Updated to meet all compliance requirements including GDPR
- Added section on Value Added roles of the CIO and CTO

Version 3.5

- Updated social networking and customer/supplier strategies
- Added two core Job Descriptions to support new digital marketplace and Omni-Commerce. Come as separate MS Word file.
  - Chief Digital Officer
  - Digital Brand Manager
- Added an eReader version of the IT Infrastructure Strategy, and Charter
- Updated to meet latest compliance requirements
- Updated all Internet HTML links

Version 3.4

- Added Job Family Classification
- Added references to policy, procedures, and electronic forms
- Updated to meet latest mandated compliance requirements
- Updated all exhibits

Version 3.3

- Updated to add a section on strategy for Omni Commerce and ERP

Version 3.2

- Updated to comply with latest ISO requirements
- Updated graphics

Version 3.1

- Added benefits section
- Updated to comply with CobiT requirements
- Added Security Management Compliance Checklist
- Added Massachusetts 201 CMR 17 Compliance Checklist
- Updated stylesheet elements

Version 3.0

- Updated stylesheet to be CSS compliant
- Updated to be HIPAA and PCI compliant
- Added CIO Job Description
- Added CIO Small Enterprise Job Description

Version 2.1

- Added section defining ISO
- Added section defining ISO 27000 standard series
- Updated template to comply with ISO 27001 and 27002
- Updated Security Process Audit Check List to comply with ISO 27001 and ISO 27002
- Corrected errata

Version 2.0

- HIPAA Audit Program Added
- ISO 177799 Security Process Audit Check List Added
- Office 2007 version Added