Edexcel Principal Learning

Information Technology

Level 3
Unit 7: Making Projects Successful

June 2013
Pre-release material

Paper Reference
IT307/01

You are not allowed to take your pre-release work into the examination.

Turn over ▶

W42029A

2/

PEARSON

FunkiPad Ltd

FunkiPad Ltd is a small business that started trading two years ago. The company was started by Sarah and Steven Smallford (the directors) and specialises in designing customised bespoke iPad accessories. The business has been a huge success and the directors need to expand the business to cope with the growing demand for their products.

As part of the expansion plans, the directors have recently leased an office space on a local business park. They have also employed ten new sales advisors increasing the existing sales team to 20 staff. The new office needs to be networked with desktop PCs and the directors have asked their IT Technician, George Peony, to project manage the process.

George has been asked to ensure that the network is future proof and can accommodate up to 15 new users over the next three years. As part of the requirement, George has been asked to upgrade the existing server to a higher specification. He has been instructed to source all of the hardware and software needed from YGH Supplies as it provides FunkiPad Ltd with a discount. YGH Supplies will also be responsible for installing the cabling in the office space.

The directors have asked George to carry out and complete the project in July, as the staff will be occupying the premises on the 5th August 2013.

FunkiPad Ltd has secured a bank loan of £35 000 for the project from Finance Bank UK.

	Task Name	Duration	Start	Finish	Predecessors
8	**Installation**	**18 days**	**Wed 03/07/13**	**Mon 29/07/13**	
9	Install cable pathways	2 days	Wed 03/07/13	Fri 05/07/13	7
10	Install cabling	2 days	Fri 05/07/13	Tue 09/07/13	9
11	Test Cabling	1 day	Tue 09/07/13	Wed 10/07/13	10
12	Install router, switches, patch panel	2 days	Wed 10/07/13	Fri 12/07/13	11
13	Test routers, switches, patch panel	2 days	Wed 10/07/13	Fri 12/07/13	11
14	Connect work stations	3 days	Fri 12/07/13	Wed 17/07/13	13,12
15	Connect Server	1 day	Fri 12/07/13	Mon 15/07/13	13,12
16	Configure server	2 days	Mon 15/07/13	Wed 17/07/13	15
17	Install Network Management software	3 days	Wed 17/07/13	Mon 22/07/13	16
18	Test Server	2 days	Mon 22/07/13	Wed 24/07/13	17
19	Test work stations	3 days	Wed 24/07/13	Mon 29/07/13	18,14
20	End of Installation	0 days	Mon 29/07/13	Mon 29/07/13	19

Gantt Chart

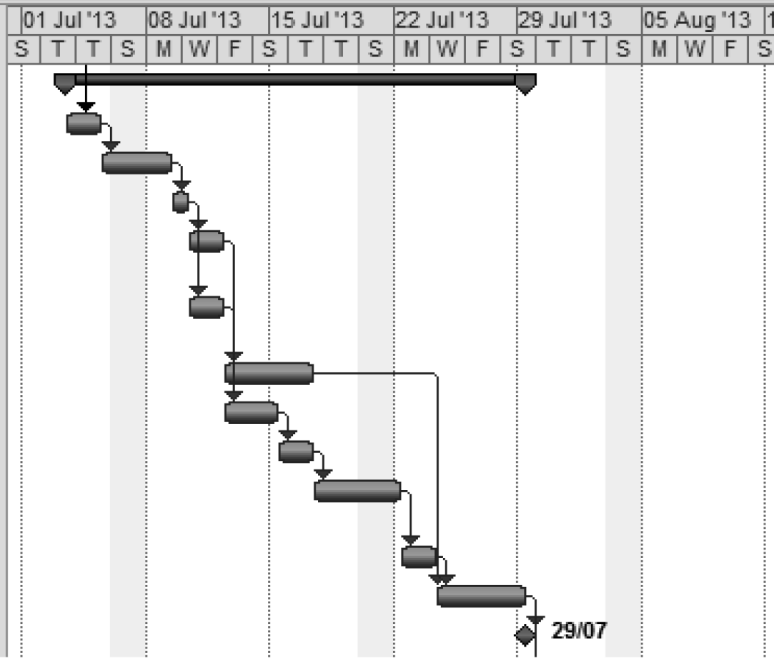

Figure 1

Extract from FunkiPad Ltd project plan

UNITED STATES DEPARTMENT OF DEFENSE

Identity Management Programme

The United States Department of Defense is a Federal Agency headquartered at the Pentagon, and includes the four branches of the armed services – Army, Navy, Air Force and Marines. The additional members of the seven uniformed services include the Coast Guard, the Commissioned Corps of the National Oceanic and Atmospheric Administration (NOAA), and the U.S. Public Health Service (PHS) Commissioned Corps. The Common Access Card Programme was created to improve security and reduce fraud by providing uniformed personnel with a secure smart card for entry to buildings, computer networks and systems.

Supplier
EDS – system design, implementation, and infrastructure maintenance; Sun Microsystems – security advice and hardware; ActivIdentity, Inc – software for card issue and use.

Timescale
The Common Access Card directive was issued in November 1999 and the first Common Access Card was issued in October 2000.

Current status
The programme has issued over ten million cards worldwide and continues to be the method used by the Department of Defense for identity assurance and Personal Identity Protection.

Key components of success

- Well-defined business and operational policies and procedures that are clearly communicated across the vendor and client communities.
- The use of industry and commercially approved standards and procedures for defining technical requirements.
- The use of commercial off-the-shelf technologies to allow a continuity of supply and the ability to procure the most cost-effective package.
- A phased, incremental deployment with scheduled review cycles to ensure that potential issues (scalability, user training, communications plan) can be analysed, updated, and then incorporated into the ongoing roll out of the deployment.

Aim

1 The United States Department of Defense (DoD) employs approximately 3.2 million military, civilian and contract personnel in more than 130 countries and 40,000 locations. It is essential for the DoD to have an effective identity system that prevents unauthorized access to its installations, IT systems and sensitive information for security. In 1999, the Deputy Secretary of Defense issued a directive to create a standard electronic identity card for military, civilian, and contract staff to enable physical access to buildings and controlled spaces, gain access to the Department's computer networks and systems, and assure identity to obtain privileges and benefits.

2 The Common Access Card programme was established to deliver an electronic smart card that contains demographic data of the user and information such as name, rank and blood type. The Common Access Card allowed business processes to be streamlined by centralising basic data into one place and assisting in the automation of manual paper based transactions.

3 The undertaking was ambitious in scale, requiring the Department to build a network of 2,000 card issuing workstations at 900 sites worldwide, to install more than one million card readers, and to issue cards to more than 3.2 million personnel.

Testing the viability of the technology and business process

4 The Department was cognisant of past government mistakes in choosing overly complex systems and custom-made technologies and chose instead to follow international and commercial standards for the Common Access Card. The two standards chosen were Java Card and GlobalPlatform. These standards offered the advantage of access to competing card vendors, thus ensuring continuity of supply if one supplier went out of business, and mixing and matching of different suppliers' software and hardware to obtain the most cost-effective package.

5 In view of the scale and technical complexity of the programme and the newness of standards for smart card technology, which were relatively immature when the programme deployed, the Department decided to test and evolve the identity card technology, and its functionality, and the process for issuing the card over a twelve month period. The first test site was established in October 2000. By mid-2001, 70 sites around the world were issuing cards. The project team used this initial phase of the roll-out to improve both the card technology and the business process.

6 The early stages of the card issuing process identified strains on the capacity of the computer systems involved. Due to unreliable connectivity between key systems, some pilot locations were unable to issue cards at certain times of day. Steps were taken to address the connectivity problem and to add redundancy and robustness to the issuance infrastructure.

7 Feedback from front line staff was used to improve the card issuing process. The programme manager visited the best performing pilot locations to consult front line staff on what worked well. This process identified some simple lessons, such as the need to clean printers thoroughly and to bolt down hardware at the issuing sites. These lessons were passed to other locations and improved their card issue performance. The consultation was also helpful in demonstrating to staff the Department's commitment to making the programme succeed.

8 Once users began using the card, many applications ran smoothly. However, as the programme scaled up and the user base grew, problems arose in achieving the key goal of meeting the DoD's mandate to digitally sign all electronic mail and other electronic documents. Downloading over 30 megabytes of Certificate Revocation List (CRL) data took over an hour to complete, resulting in loss of productivity. Also to avoid waiting, many users circumvented the system and used webmail, causing significant security concerns. To address this, the programme team identified the need for a new validation protocol – Distributed Online Certificate Status Protocol – which reduced the validation time as well as increasing security.

Addressing user concerns

9 Programme success depended on obtaining user buy-in. A comprehensive public relations plan was developed that outlined the benefits of using the card and ensured that all users were aware of the card prior to its arrival. The early stages of the implementation identified that users were uncertain about whether they were using the card correctly. To address this, the project team set up a training programme for users and improved helpdesk assistance.

Realising the benefits

10 The Common Access Card programme has delivered efficiency gains. The time taken to issue an identity card has been reduced from hours to 15 minutes through reducing the paperwork involved and simplifying card issuing arrangements. This efficiency benefit will continue with each card issued to new staff or reissued by existing staff.

11 The card enables army divisions to assess deployment readiness in minutes rather than hours. Previously, army personnel were required to present their finance, personnel, and medical records to twelve different contact points and waited in line for their details to be processed to determine if they were equipped to go on manoeuvres. Using the Common Access Card, all the required information can now be read automatically from a single interaction and deployment readiness can be verified almost instantaneously. The Department of Defense estimated that a typical infantry division can save 30,000 man-hours a year by using the smartcard rather than the paper-based process.

12 The Department of Defense has identified that the card technology can deliver further savings and more functionality without needing to issue new cards. For example, the technology has already been extended to support a travel system that allows users to sign their travel vouchers electronically, eliminating the need for paper based processes. The next technological challenge will be the incorporation of biometric data into the card. This capability is currently under development and will be deployed during 2006.