European Commission TEMPUS

e-Government Lifelong Learning Consortium Project

BIRZEIT UNIVERSITY

Palestinian E-Government Needs Assessment: Skills Analyses and Training Program

(Deliverables: D1.1, D2.1, D3.1)

Mustafa Jarrar (BZU),Majd Ashhab (BZU), Radwan Tahboub (PPU), Romain Robert (UoN)
with contribution from
Mahmoud Saheb (PPU), Ismail Romi (PPU), David Chadwick(TT), Mohammad Jubran (BZU)

Abstract

This report identifies the skills needed to implement and deploy an e-government framework, focusing on the interoperability, security, and legal needs. The report also suggests a training program of six training tutorials, or alternatively, six academic courses, that are necessary to build these skills.

The methodology used to identify the missing skills was analytical. That is, the Palestinian e-government architecture was studied and analyzed and the skills and know-how needed to implement and deploy this were identified in consultation with the governmental and private sectors. We then estimated the present skills and know-how of the Palestinian governmental and private sectors. From the identified present skills and required skills, the missing skills were deduced. This allowed us to derive the Intended Learning Outcomes that are required for the suggested training program.

Document Identifier:	Pal-Gov_Needs_Assessment
Project:	Palestinian e-Government Academy
Version:	Ver 0.18
Publication Date	24/7/2011
Status	Final
Distribution	Public

The Project:

Project Number: 511159-TEMPUS-1-2010-1-PS-TEMPUS-JPHES
Project Short Name: Pal-Gov
Project Full Name: e-Government Lifelong Learning Consortium

Project Consortium:
This document is part of a project funded by the TEMPUS IV program of the Commission of the European Communities, grant agreement 511159-TEMPUS-1-2010-1-PS-TEMPUS-JPHES.

1. Birzeit University, Palestine (Coordinator)
2. Palestine Polytechnic University, Palestine
3. Palestine Technical University, Palestine
4. University of Trento, Italy
5. Vrije University Brussels, Belgium
6. University of Namur, Belgium
7. True Trust, UK
8. University of Savoie, France
9. Ministry of Telecom and Information Technology, Palestine
10. Ministry of Interior, Palestine
11. Ministry of Local Government, Palestine

Document Track Changes

Version	Date	Author(s)	Changes
V0.01	19/11/2010	Mustafa Jarrar	Document Creation
V0.02	5/1/2011	Mustafa Jarrar	First Draft
V0.03	25/1/2011	Majd Ashhab	Insert Methodology Section
V0.04	29/1/2011	Mustafa Jarrar	Revision
V0.05	2/3/2011	Radwan Tahboub	Initial update in the Security Section
V0.06	11/3/2011	David Chadwick	Comments and corrections
V0.07	25/3/2011	Romain Robert	Legal Informatics Sections
V0.08	1/4/2011	Radwan Tahboub	Initial update in the Security Section
V0.09	3/4/2011	Mohammad Jubran	Revision and corrections for the Security Section
V0.10	18/4/2011	Mahmoud Saheb	Adding modified Interoperability Tutorials and new courses
V0.11	25/4/2011	Radwan Tahboub	Final Draft
V0.12	29/4/2011	Ismail Romi	Adding Legal Informatics ILO's, Tutorials, and Course
V0.13	25/4/2011	Radwan Tahboub	Final review after legal part additions and before sending to quality control.
V0.14	4/5/2011	Majd Ashhab	Review and corrections
V0.15	10/5/2011	Radwan Tahboub	Adding skills / ILOs tables
V0.16	12/5/2011	Mahmoud Saheb	QC final revision
V0.17	21/72011	Feras Melhem	Adding The Final Legal Informatics ILO's, Tutorials, and Course
V0.18	24/7/2011	Mahmoud Saheb	QC Final

Table of Contents

1. Methodology

A structured and well defined methodology was pursued in order to identify the skills and the know-how needed to implement and deploy the e-government architecture and then use these identified skills to develop the outlines of the tutorials and the academic courses that the Palestinian e-Government Academy will offer. In all steps of our methodology, significant participation of key people from academia, government and private sector was present in order to reassure and confirm the outcomes of every step.

The methodology we pursued to identify the necessary skills and know-how needed to implement and deploy the e-government architecture is an analytical methodology. Needs' analysis has been conducted to bridge the gap between the trainee's initial training experiences and the actual knowledge and skills needed for e-government implementation:

Step one: **Identify the *general* missing skills and know-how**:

- Study of the proposed e-government architecture and its components and frameworks.
- Identify the skills and knowledge needed to implement and deploy the e-government architecture and framework
- Observe the existing skills and knowledge of Palestinian government and private sector employees
- Deduce the missing skills and knowledge in the Palestinian governmental and private sectors in view of the proposed e-government architecture and framework.
- Conduct several meetings with the Palestinian government and universities to assure whether the general skills audit is comprehensive.

The result is a set of missing skills, in general terms.

Step two: **Derive the Intended Learning Outcomes:**

- Elaborate the set of general missing skills to arrive at a set of more specific skills, taking into account the specific and technical details and knowledge that one needs in order to implement and deploy the e-government architecture and frameworks.
- Assure whether this set of specific skills is realistic through interviews and discussions with the governmental and private sectors.

The result is a set of specific skills that are seen as learning objectives of the training program proposed in the next step.

Step three: **Design the training program:**

- Derive the set of topics for the training program based on the results of the previous step (learning outcomes).

- Group the topics thematically to produce a training program of six tutorials to train the public and private sector, or alternatively, into six academic courses that can be introduced to the curricula of the universities.
- Assure the coherence and currency of the program and its topics by intensive discussion and review with the EU and Palestinian scientists.
- Assess the proposed topics in cooperation with the EU partner universities.

Following this methodology, it was assured and verified that the general and specific skills are realistic, and that the suggested learning objectives and topics are aligned with the e-government architecture and frameworks. Moreover, the suggested learning outcomes and topics reflect the agreements that emerged from several meetings and discussions with the partner ministries and universities.

2. The Palestinian e-Government Architecture

This section describes and analyzes the architecture of the Palestinian e-government, its basic building blocks, functionalities, and frameworks. The skills and the needed know-how to implement this architecture are stated in general terms. A discussion of these skills in detail and their mapping into learning outcomes will be discussed later in this report.

The following diagram depicts the most recent system architecture of the Palestinian e-government [7], which has been developed in cooperation with the Estonian government. The architecture connects all ministries together through a *government service bus*, called "x-road Palestine". This service bus, with the other components, represents standard *service oriented architecture* [2], with an emphasis on the provision of secure services. It should be noted that this architecture is not yet implemented, but there is a general consensus about it among most governmental bodies, especially the Ministry of the Telecommunication and Information Technology [1].

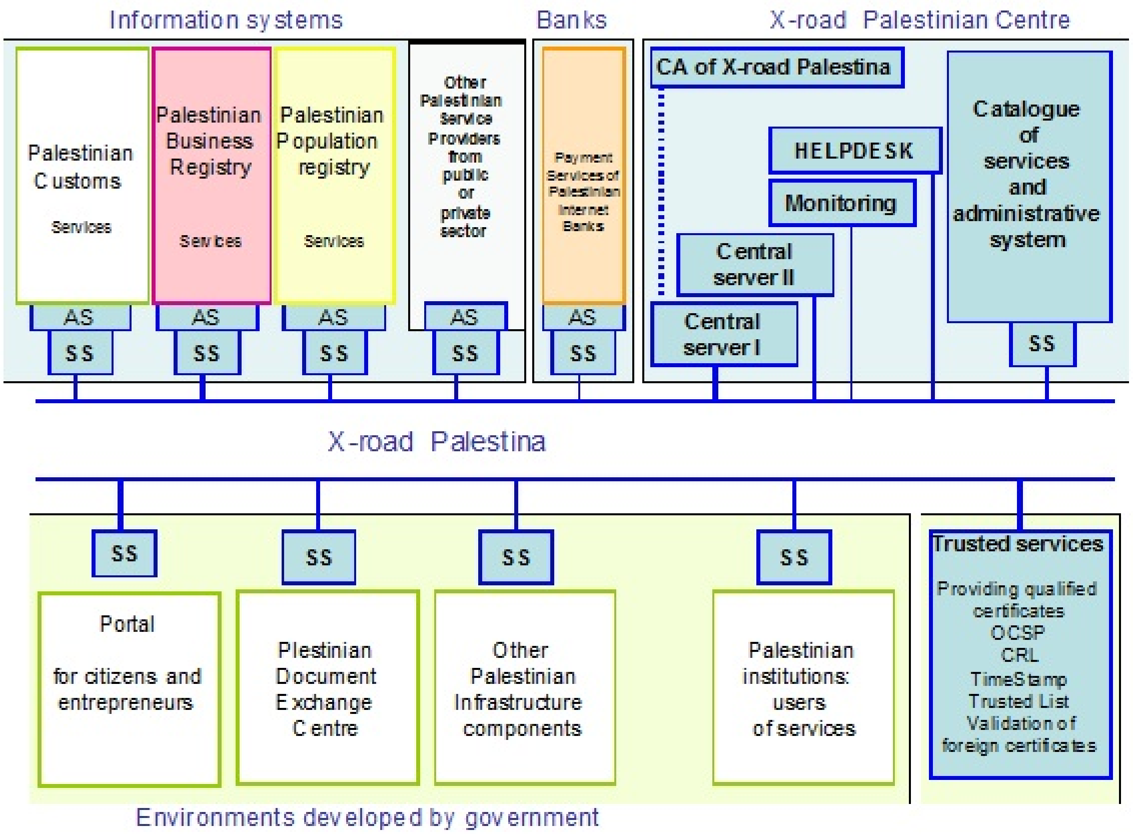

Information systems
Banks
X-road Palestinian Centre
Palestinian Customs
Services
Palestinian Business Registry
Services
Palestinian Population registry
Services
Other Palestinian Service Providers from public or private sector
Payment Services of Palestinian Internet Banks
AS
SS
CA of X-road Palestina
HELPDESK
Monitoring
Central server II
Central server I
Catalogue of services and administrative system
X-road Palestina
Portal
for citizens and entrepreneurs
Plestinian Document Exchange Centre
Other Palestinian Infrastructure components
Palestinian institutions: users of services
Trusted services
Providing qualified certificates
OCSP
CRL
TimeStamp
Trusted List
Validation of foreign certificates
Environments developed by government

Figure 1. The Palestinian e-Government Architecture

Figure 1 Legend. SS=security server
AS = application server
CA = certification authority
OCSP= online certificate status protocol

CRL = certificate revocation list

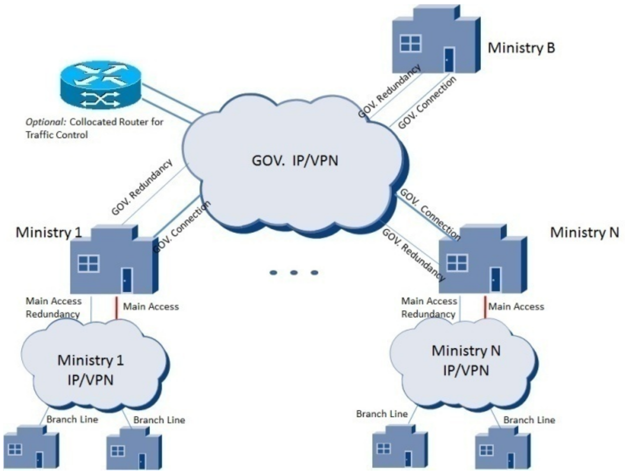
Public services can be accessed by citizens or entrepreneurs through the portal component. The portal is nothing more than an interface to the e-government system. It allows users first to login and authenticate themselves through smart-card and/or passwords; the portal then provides the list of services that the authenticated user is allowed to access. When a user selects a service, say “renew driving license”, the portal communicates with the other servers, for example with the server of the ministry of transportation who is the provider of this service to make sure that this driving license can be renewed. Then, the server communicates with the server of the ministry of interior to get the recent photo and address of this user. After that, it communicates with the server of the ministry of health to assure that the user has a valid vision test, if needed. After this interaction with the other servers, the portal asks the user to confirm and proceed to the payment service, and so on.

Although such interoperations between servers is not visible to the user and seems simple, however several *frameworks* should be established to enable these interoperations, especially because these servers are not located in one place or operated by one organization. Each organization develops and operates its services and data (accessed through its Adapter server, AS). An organization can be a ministry, a governmental agency like the Lands Authority or the Monetary Authority, or a private firm like banks, insurance companies, chambers of commerce or telecom operators. In Palestine, there are 23 ministries, 55 governmental agencies, and many private firms that may all join the e-government at a certain stage.

Hence, the e-government is simply an *orchestration* between all interoperating institutions. Specifically, five frameworks are needed to implement the aforementioned e-government architecture and to orchestrate the interoperations between all institutions; (i) infrastructure framework, (ii) security framework, (iii) interoperability framework, (iv) legal framework, and (v) policy framework.

2.1Infrastructure Framework

This framework is concerned with the network needed to connect all ministries. For example, should the ministries be connected through the Internet or through a closed network? Who will manage this network and which technical communication protocols should be used? In Palestine, a closed *government network* called GovNet has been established already to connect all governmental parties, and this network will be used as an infrastructure framework for the e-government. The topology and usage assumptions are presented below.



- *Palestinian GovNet will operate as a public network.*
- *Principles of GovNet:*
  - *Every governmental institution has the right, though not obligation, to use GovNet.*
  - *The use of the backbone network is recommended to be financed centrally from the state budget, and all* institutions can use it freely*.*
  - *Each institution is responsible for the security of its local network.*

Figure 2. The Infrastructure Framework: *GovNet Topology and usage assumptions*.

2.2Security Framework

After establishing the network between governmental institutions, this network needs to be secure: both point to point network security and end-to-end service security. In order to achieve this objective, all the following issues should be integrated and guaranteed in one way or another:

- Data Confidentiality: All traffic between ministries platforms and user platforms should be confidential.
- Data Integrity: It should be impossible to change the exchanged data either by hackers or by communication network errors without it being detectable.
- Authenticity: when Ministry A receives a message from ministry B, there should be no doubts for ministry A that ministry B really is the sender; that is; no one can steal the identity of B.
- No surreptitious forwarding: when Ministry A receives a message from ministry B, there should be no doubts for ministry A that it is the intended recipient of the message, that is, no one has forwarded a message that was destined for ministry X, to ministry A, without ministry A being able to tell that this was the case.
- Non-repudiation: ministry B cannot deny sending the message to ministry A.
- Access Control: Only authorized people can do privileged actions.
- Accounting and Logging: All actions should be logged and can be audited at any later time. The audit log should be tamperproof to stop attackers covering their tracks.
- Availability: All Servers, Services, Networks, communications systems, and other computing resources should be highly available with minimum risks of unscheduled downtime.

To deal with these issues, the following services are needed:

- Intrusion detection and prevention.
- Malicious software and virus protection.
- Denial of service and distributed denial of service detection and prevention.
- Firewall systems.
- Risk assessment and management.
- Policy making and enforcement.
- Training and awareness building.

Missing Knowledge and Skills:
For all:

- Understand the types of risks and threats from being connected.
- Understand security standards and policies including risk assessment and management
- Be aware of the threats of connecting to the internet and using web applications and social networks
- Ability to protect themselves and applications from security threats

For IT professionals:

- Ability to design, implement and deploy user authentication services.
- Ability to design, implement and deploy end-to-end security systems.
- Ability to design, implement and deploy authorization services.
- Ability to design, implement, and deploy confidentiality services.,
- Ability to design and deploy security policies

As shown in the architecture above, ministries can communicate only through security servers. That is, each ministry is connected to the x-road through a *security server* (SS). For example, when ministry A sends a message to ministry B, Ministry A sends this message first to its own security server, which will encrypt and digitally sign this message, and send it to the security server of ministry B, which will decrypt this message and process the digital certificate to verify the sender (ministry A) and the message integrity, it will also confirm that it is the intended recipient. To allow this secure communication, not only the security servers, but also the certification authority, central servers, and Trusted Services should be established. That is, in order to allow servers to digitally sign a message a public key infrastructure PKI should be established which also needs several other common services such as OCSP. Furthermore, in order to insure the robustness and integrity of this security framework, each message sent out from an institution is hashed with a time stamp and this hash is sent to the central audit bus so that one may subsequently monitor/investigate whether the message was sent or not.

The above description emphasizes the security between institutions' servers. However, the security between an end-user and the portal might be achieved through the use of the HTTPS protocol and soft-certificates. Users may login to the portal and authenticate themselves using simple passwords, one-time passwords, smart cards, one-time codes sent promptly to their mobiles, or a combination of these.

Although it is not visible in the architecture above, it is assumed that institutions strictly follow best security practice in order to make sure that their and other's data is secure even with offline modes.

2.3Interoperability Framework

Establishing a secure network as described above, does not mean that institutions can understand each others' messages. That is, an interoperability framework is needed to mediate between the technical, organizational, and semantic diversity of the institutions. For example, institutions should agree on and use the same communication protocols, same format of the exchanged messages, same semantics of the used vocabularies, same data structure, same identities of entities, and so on.

The following diagram depicts the *Interoperability Framework* [8], which is being developed at the Ministry of Telecommunication and Information Technology.

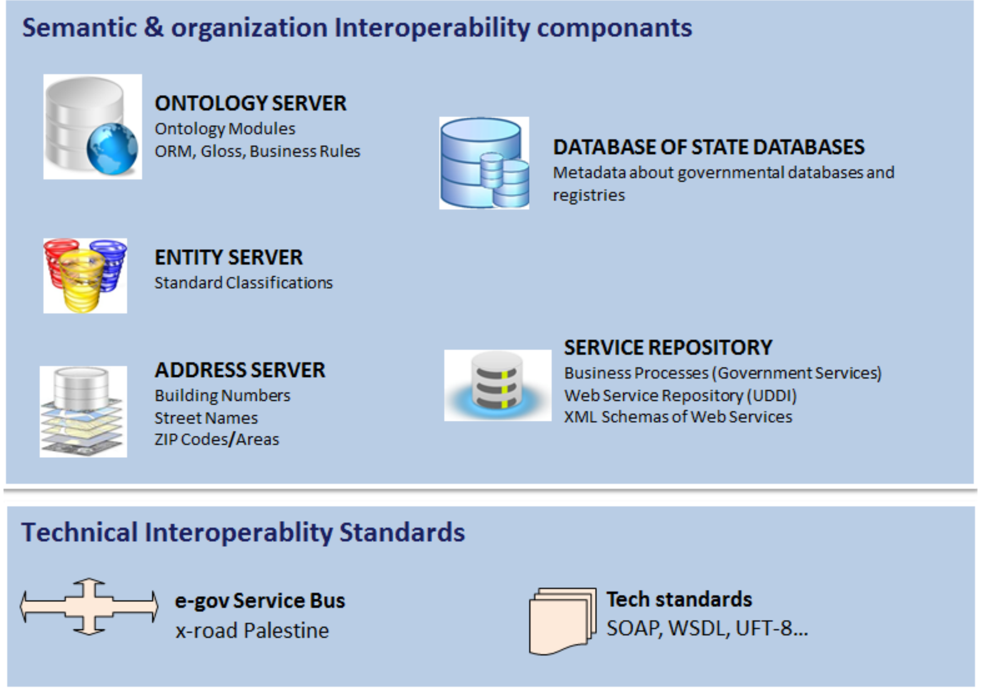

Semantic & organization Interoperability componants
ONTOLOGY SERVER
Ontology Modules
ORM, Gloss, Business Rules
DATABASE OF STATE DATABASES
Metadata about governmental databases and registries
ENTITY SERVER
Standard Classifications
SERVICE REPOSITORY
Business Processes (Government Services)
Web Service Repository (UDDI)
XML Schemas of Web Services
ADDRESS SERVER
Building Numbers
Street Names
ZIP Codes/Areas
Technical Interoperablity Standards
e-gov Service Bus
x-road Palestine
Tech standards
SOAP, WSDL, UFT-8...

Figure 3. The Palestinian Interoperability Framework.

As the *Technical Interoperability Standards* part of the above figure indicates, the "x-road Palestine" is a standard service oriented architecture [2], in which institutions communicate through *web services [2], using the SOAP* protocol [3]. Web services are described using the standard Web Service Description Language WSDL [4].

That is, when implementing a public service, e.g., "renew driving license", this service is decomposed into atomic tasks, and each task is implemented as a web service. Each institution provides a set of web services that can be used by other institutions. For example, the Ministry of Interior may provide a web service to allow other institutions to look up citizen profiles, the Ministry of National Economy may provide a web service to allow looking up company information, and so.

Missing Knowledge and Skills:

- Ability to integrate services in a (de)centralized manner
- Ability to integrate and fuse heterogeneous data in a (de)centralized manner

The above described service oriented architecture is only one technique to achieve data and service integration. This solution allows the integration to be achieved in a decentralized manner through web services. However, there are other techniques to data integration that might be used offline or locally, inside an institution or between certain institutions; such techniques include LAV or GAV schema integration [5] and Data Fusion [6].

Missing Knowledge and Skills:

- How to build, engineer, and use ontologies.
- How to engineer multilingual knowledge and its lexical semantics

As the semantic and organizational components in the above figure indicate, there are five servers which are core to achieving data and service integration:

The Ontology Server: The server is a library of *e-government ontology* modules. The e-government ontology provides a shared description of the terminology (concepts and their interrelationships) that are communicated in the government domain; such that, ministries sharing (i.e., committing to) this ontology can interoperate meaningfully. That is, all terminology used in the web services is mapped to (i.e. commits to) this ontology. The government ontology can be regarded as a framework (/standard) that consists of the agreed-upon vocabulary (i.e. naming), meaning, data structure, and business rules, pertaining to the data exchanged in e-government services. The e-government ontology needs to be lexicalized in two languages at least; Arabic and English.

The Entity Server provides the standard codes and multilingual names of all entities shared between institutions; such entities can be countries, currencies, genders, material statuses, religions, and so on. When an institution exchanges data with another institution, the exchanged data must conform to the codes provided in the Entity Server. The entity server can also provide *identity mapping*. For example, when a person or a car has different identities across different institutions, these identities can be mapped to each other, and this mapping is published and shared through the Entity Server.

Missing Knowledge and Skills:

- How to resolve and manage entity identities

The Address Server is a GIS-enabled database of all addresses. When an institution exchanges data with another institution and this data contains an address of a citizen or an organization, this information must conform to the addresses published at the Address Server; such that all addressing information become integrated across institutions.

The Database of State Databases is a server that provides a general description about all databases of all institutions. Its main goal is to provide information about what data elements are stored in or registered in which institution. This allows institutions to know who is responsible on registering what data, thus reducing redundancy.

Missing Knowledge and Skills:

- How to describe database schemes at the conceptual level.
- Databases: How to build data dictionaries and describe data semantics

The Service Repository is a catalogue of (a) all public services, which we scientifically call *business processes*; and (b) all web services, which implement the business processes. The first component is *not* a flat list of all business processes names, but rather, a full description (formal and informal) of each process. The formal description of a service includes it's As Is and To Be models. All processes are also categorized according their nature, provider, and consumer. The second component of the service repository includes metadata and description of the web services that are needed to implement the business processes. This component could be used as a UDDI.

Missing Knowledge and Skills:

- Process Modeling: How to identify, model, and (re-) engineer business processes.

2.4 Legal Framework

After establishing the secure network and ensuring that institutions are able to exchange data messages meaningfully, a legal framework is needed in order to regulate these interoperations. For example, the exchanged information should be legally framed, in order to ensure the legal coherence of these e-government services and the various rights and obligations of the administrations and the citizens regarding the access to e-government services and data. In addition, since personal data protection and privacy issues are at stake when processing personal information, a legal framework addressing the protection of personal data and privacy should be drafted.

Among others, three main legal instruments could provide a viable solution to enable e-government services to work in a coherent legal framework:

Digital Signature Act

Such a legislation would aim at providing a legal framework to regulate the legal value of electronic communications and transactions, taking into account the existing requirements needed for a transaction to be legally accepted under Palestinian law, the legal requirements and procedures of a valid digital and handwritten signature, the management and legal value of digital identities and authentication of people and organizations, PKI infrastructure and certification authorities, among other issues.

Missing Knowledge and Skills:

- IT people: understanding the basics of law and the Palestinian legal system.
- IT people: understanding the art of formulating regulations
- Lawyers: understanding the concept of digital signature, PKI, digital identities, and other security technologies.
- IT/lawyers: Understanding the state of art on related acts in other countries.

Privacy and Data Protection Act

Such legislation, inspired from the European Directive 95/46 on the protection of individuals with regard to the processing of personal data would create a legal framework under which the governmental administrations and private individuals will process the personal information that they collect about the individuals. Such a regulation would provide for the basic principles to be met in case of processing of personal data: definition of the precise purposes for which a processing can occur; description of the legal basis allowing the processing of personal data; obligation to inform the data subjects about various aspects of the processing of their data; right of the data subject to access/modify or rectify the data; adoption of security measures to avoid accidental loss, damage, destruction of data or unauthorized access; transfer of data to another organization/individual, inside or outside the country; adoption of specific protection for sensitive data such as data relating to health, criminal records, race, ethnic origins, or revealing philosophical, religious or political opinions.

Missing Knowledge and Skills:

- IT people: understanding the basics of law and the Palestinian legal system.
- IT people: understanding the art of formulating regulations
- Law people: understanding the concept of storing and processing data in the digital world.
- IT/law people: Understanding the state of art on related acts in other countries.

Missing Knowledge and Skills:

- IT people: understanding the basics of law and the Palestinian legal system.
- IT people: understanding the art of formulating regulations
- Law people: understanding the concept of a database, standard classifications, codes, and naming.
- IT/law people: Understanding the state of art on related acts in other countries.

Information Systems Act

This act would aim at regulating the functioning of public databases, defining under which circumstances a public ministry department or other public entity may collect process and use data, or share it (or refuse to share it) with other public or private bodies, the legal value of an information held by a public institution, the right for the citizen to update his data or to rely on the existing data retained by the administration, the security measures and standards that must be adopted to protect the data, the possibility to create interconnection between various existing databases, the management of the various access rights by the designated public or private agents.

2.5 Policy Framework

After establishing the secure network and enabling institutions to interoperate meaningfully and legally, a policy framework is needed to guide these institutions to follow the national priorities and strategies. For example, what e-government services to provide, not provide, and which are more important than others; to whom services should be provided (e.g., Palestinians with green ID cards, blue cards, foreigners, refugees); and so on.

3. Tutorials and Courses Intended Learning Outcomes

This section takes each of the "*missing knowledge & skills*" identified in the previous section, and provides a set of more *specific skills*. That is, in this section, we map the general to the more specific skills. These specific skills will be used in the next section as *Intended Learning Outcomes (ILOs)* for the proposed tutorials and academic courses.

To confirm that the general and specific skills are realistic, not only are they aligned with the e-government architecture and frameworks as shown in the previous section, but also they reflect the agreements that emerged from several meetings and discussions with the partner ministries. The following is a summary of the specific skills and knowledge that are necessary to implement and deploy the e-government Architecture. They are arranged into 3 areas: interoperability, security, and legal informatics.

3.1Interoperability Intended Learning Outcomes

Ability to integrate services in a (de)centralized manner

3a3: Knowledge: Explain the concept of service oriented architectures.
3a1: Knowledge: Demonstrate knowledge of the fundamentals of middleware.
3a2: Knowledge: Describe the concepts behind web service protocols.
3a4: Knowledge: Explain the concept of an enterprise service bus.
2a2: Knowledge: Understand the notation of XML.
2a3: Knowledge: Demonstrate knowledge about querying techniques such as XPath.
2b1: Skill: Represent data in XML format.
2b3: Skill: Manage and query data represented in XML.
3b1: Skill: Design, develop, and deploy applications based on the Service Oriented Architecture (SOA).
3c1: Skill: Setup, Invoke, and deploy web services using an integrated development environment.
3c2: Skill: Construct and use REST and SOAP messages for web services communication.
3b3: Skill: Use WSDL to describe web services.
3c3: Skill: Publish WSDL service interfaces in UDDI.
3b2: Skill: Use Business Process Execution Language (BPEL).

Ability to integrate and fuse heterogeneous data in a (de)centralized manner

2b4: Skill: Demonstrate knowledge about Integration and fusion of heterogeneous data.
11a3: Knowledge: Explain and demonstrate the concepts of data integrity and business rules.
2a4: Knowledge: Explain the concepts of identity management and Linked data.
2a1: Knowledge: Describe tree and graph data models.
2a3: Knowledge: Demonstrate knowledge about querying techniques for data models as SPARQL and X-Path.
2b4: Skill: Integrate and fuse heterogeneous data.
4b5: Skill: Match multiple ontologies (or Schemes).
11b2: Skill: Analyze entity identity at the application and domain levels.
2b3: Skill: Manage and query data represented in RDF, XML, OWL.
2c1: Skill: Using Oracle Semantic Technology and/or Virtuoso to store and query RDF stores.

Build and engineer ontologies of good quality.

4a1: Knowledge: Demonstrate knowledge of what is an ontology, how it is built, and what it is used for.
11a1: Knowledge: Demonstrate knowledge of conceptual modeling notations and concepts.
11a2: Knowledge: Demonstrate knowledge of Object Role Modeling (ORM) methodology.
4a3: Knowledge: Describe the differences between an ontology and a schema, and an ontology and a dictionary.
4a2: Knowledge: Demonstrate knowledge of ontology engineering, evaluation, and matching.
2a2: Knowledge: Understand the notation of XML, RDF, RDFS, and OWL.
4b1: Skill: Develop quality ontologies.
11b1: Skill: Analyze application and domain requirements at the conceptual level, and formalize it using ORM.
4b4: Skill: Formulate quality glossaries.
2b2: Skill: Describe data semantics using RDFS and OWL.
4b2: Skill: Tackle ontology engineering challenges.
11b5: Skill: Detect and resolve contradictions and implications at the conceptual level.
11b4: Skill: Optimize, transform, and (re)engineer conceptual models.
4b5: Skill: Match multiple ontologies.
4c1: Skill: Use ontology tools.
11c1: Skill: Using ORM modeling tools (Conceptual Modeling Tools).
2c2: Skill: Using Protégé and/or TopBraid to author RDFS, and OWL.

Engineer multilingual knowledge and its lexical semantics

4a4: Knowledge: Explain the concept of language ontologies, lexical semantics and multilingualism.
4b3: Skill: Develop multilingual ontologies.
4c2: Skill: (Re)use existing Language ontologies.

Resolve and manage entity identities.

2a4: Knowledge: Explain the concepts of identity management and Linked data.
11b2Skill: Analyze entity identity at the application and domain levels.

Describe database schemes at the conceptual level.
Build data dictionaries and describe data semantics.

11a1: Knowledge: Demonstrate knowledge of conceptual modeling notations and concepts.
11a3: Knowledge: Explain and demonstrate the concepts of data integrity and business rules.
11b1: Skill: Analyze application and domain requirements at the conceptual level, and formalize it using ORM.
4b4: Skill: Formulate quality glosses.

Identify, model, and re-engineer business processes.

12a1: Knowledge: Demonstrate knowledge of business process modeling notations and concepts.
12a2: Knowledge: Demonstrate knowledge of business process modeling and mapping.
12a3: Knowledge: Demonstrate understand of business process optimization and re-engineering.
12b1: Skill: Identify business processes.
12b2: Skill: Model and map business processes.
12b3: Skill: Optimize and re-engineer business processes.
12c1: Skill: Using business process modeling tools, such as MS Visio.

3.2Security Intended Learning Outcomes

This tutorial is designed to provide the participants with: an understanding of the concepts underlying Secure Information Systems, experience in the use of security tools and techniques to build secure models, and hands-on experience in the design and implementation of secure systems. Participants completing this tutorial should be able to demonstrate the following learning outcomes:

Security Learning Objectives

a) Understand the importance of taking a systems wide approach to maintaining information security, and the balance between risk and expenditure.
b) Have an understanding of the threats faced by computer operating systems, applications and networks (especially the Internet) and the various countermeasures that can be used;
c) Have a basic understanding of the algorithms used in cryptography;
d) Understand the motivation, design, operation and management of modern systems for encryption, authentication, authorization and identification.
e) Have an understanding of the various techniques used in identity management;
f) The ability to analyze the information security requirements of an organization.
g) Skills to use the appropriate software tools, techniques and packages to produce and develop security systems especially in the area of authentication.
h) Be able to make informed choices of the appropriate security measures to put into place for a given network, operating system or application;
i) Be able to undertake practical exercises related to securing computer systems;

A: Knowledge and Understanding

a1: Define the different risks and threats from being connected to networks, internet and web applications.

a2: Defines security standards and policies.

a3: Recognize risk assessment and management

B: Intellectual Skills

b1: Illustrate the different risks and threats from being connected.

b2: Relates risk assessment and management to e-government model.

b3: Design end-to-end secure and available systems.

b4: Design integral and confidentiality services.

b5: Design user authentication and authorization services.

b6: Develop security policies.

C: Professional and Practical Skills

c1: Deploy and configure a secure system to protect their computing resources.

c2: Configure an end-to-end secure and available system using Apache.

c3: Configure integral and confidentiality services using integrity and confidentiality algorithms and protocols.

c4: Configure user authentication and authorization services using LDAP and SSL certificates.

c5: Implement a federated Identity Management to e-government model.

D: General and Transferable Skills

d1: Communication and team work.

d2: Systems configurations.

d3: Analysis and identification skills.

In the following tables, a list of each missing competency and the ILOs is presented:

Understand the types of risks and threats from being connected.

a1: Knowledge: Define the different risks and threats from being connected to networks, internet and web applications.
a2: Knowledge: Defines security standards and policies.
a3: Knowledge: Recognize risk assessment and management
b1: Skill: Illustrate the different risks and threats from being connected.
b2: Skill: Relates risk assessment and management to e-government model.
b6: Skill: Develop security policies.
c5: Skill: Implement a federated Identity Management to e-government model.

Understand security standards and policies including risk assessment and management

a1: Knowledge: Define the different risks and threats from being connected to networks, internet and web applications.
a2: Knowledge: Defines security standards and policies.
a3: Knowledge: Recognize risk assessment and management
b1: Skill: Illustrate the different risks and threats from being connected.
b2: Skill: Relates risk assessment and management to e-government model.
b6: Skill: Develop security policies.
c5: Skill: Implement a federated Identity Management to e-government model.

Be aware of the threats of connecting to the internet and using web applications and social networks

a1: Knowledge: Define the different risks and threats from being connected to networks, internet and web applications.
a2: Knowledge: Defines security standards and policies.
a3: Knowledge: Recognize risk assessment and management
b1: Skill: Illustrate the different risks and threats from being connected.
b2: Skill: Relates risk assessment and management to e-government model.
b6: Skill: Develop security policies.
c5: Skill: Implement a federated Identity Management to e-government model.

Ability to protect themselves and applications from security threats

a2: Knowledge: Defines security standards and policies.
b2: Skill: Relates risk assessment and management to e-government model.
b6: Skill: Develop security policies.
c1: Skill: Deploy and configure a secure system to protect their computing resources.
c2: Skill: Configure an end-to-end secure and available system using Apache.

Ability to design, implement and deploy user authentication services.
Ability to design, implement and deploy end-to-end security systems.
Ability to design, implement and deploy authorization services.
Ability to design, implement and deploy confidentiality services.

a2: Knowledge: Defines security standards and policies.
b3: Skill: Design end-to-end secure and available systems.
b4: Skill: Design integral and confidentiality services.
b5: Skill: Design user authentication and authorization services.
c1: Skill: Deploy and configure a secure system to protect their computing resources.
c2: Skill: Configure an end-to-end secure and available system using Apache.
c3: Skill: Configure integral and confidentiality services using integrity and confidentiality algorithms and protocols.
c4: Skill: Configure user authentication and authorization services using LDAP and SSL certificates.

Ability to design and deploy security policies.

a1: Knowledge: Define the different risks and threats from being connected to networks, internet and web applications.
a2: Knowledge: Defines security standards and policies.
a3: Knowledge: Recognize risk assessment and management
c5: Skill: Implement a federated Identity Management to e-government model.

3.3 Legal Framework of New Technologies

This section provides the participants with an understanding of the Legal Framework of New Technologies concepts, data protection issues in e-government projects, ways of ensuring legal certainty and validity to e-government transactions, and coherence between e-government services.

Legal Framework of New Technologies Objectives

a) Understanding data protection issues in an e-government project
b) Ensuring legal certainty and validity to e-government transactions
c) Ensuring coherence between e-government services

A: Knowledge and Understanding:

a:1 understand the legal frame for access management
a2: Enforcing security management through internal regulation
a3: Understanding the current non electronic evidence law
a4: Understanding the legal framework for digital signature, certificate and third party certification
a5: Understanding the general framework for e-government transfer of information
a6: Understand the importance of policy making in the legislative process
a7:Inhance knowledge on ethics related to digital systems
a8: Wide the awareness of students & lawyers to the best practices related to IP laws & applications
a9: Widen the knowledge of privacy and data protection
a10 Enhance general understandings of e-commerce
a11: Enhance knowledge of e-contract
a.12: Enhance and understand Cybercrime
a.13 Understanding of e-archiving
a.14: Develop knowledge about international as well as EU best practices and standards

B: Intellectual Skills:

b1: Ensure public transparency of the processing of data.
b2: Ensure the workability of a e-government service

C: Professional and Practical Skills:

c1: Control of the processing of personal data by public bodies.
c2: Ensuring international transfer of data
c3: Ensuring validity of e-signature
c4: Assessing the legal admissibility of an electronic document
c5: Assessing the need for a digital signature
c6: Managing the relationship between the citizens and the public bodies in charges of e-services ?

D: General and Transferable Skills:

d1: Team Work.
d2: Governmental legal issues.
d3: Analysis skills

4. The Proposed Training Program

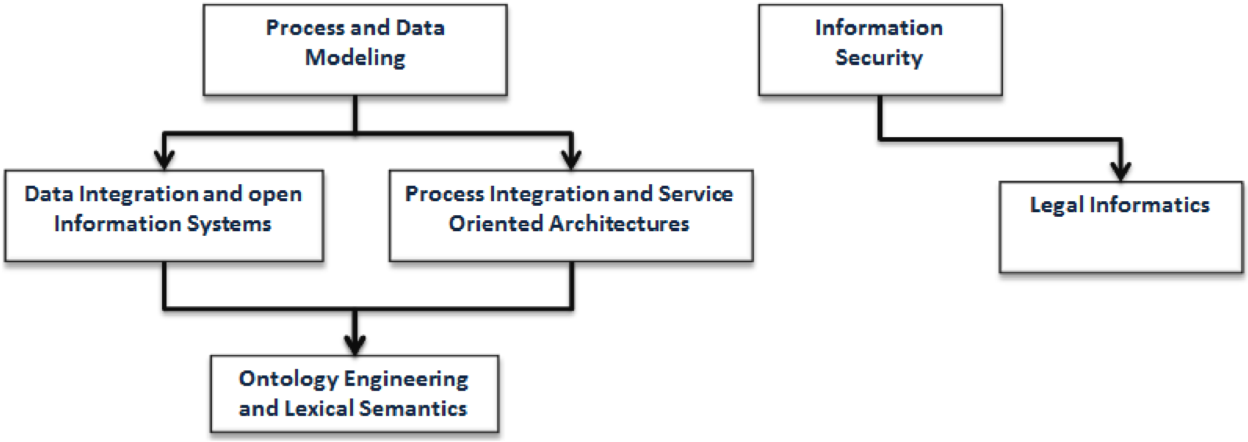
This section proposes a program of six professional training tutorials, which aims to increase the capacity of Palestinian society (both public and private sectors) with state-of-the-art knowledge for building and deploying e-government services. These tutorials are split into three main thematic areas, as follows:

Interoperability Area (4 tutorials, target trainees are IT people).
Security Area (1 tutorial, target trainees are IT people).
Legal-informatics Area (1 tutorial target trainees are law and IT people).

To provide maximum knowledge, these tutorials are designed to be followed by people with at least a 4-year degree in Information Technology or a three year degree in Computer Science, and with good practical skills and knowledge on databases, Java and UML, networking protocols and Web Programming. People with a 4-year degree in law can follow the legal informatics tutorial.

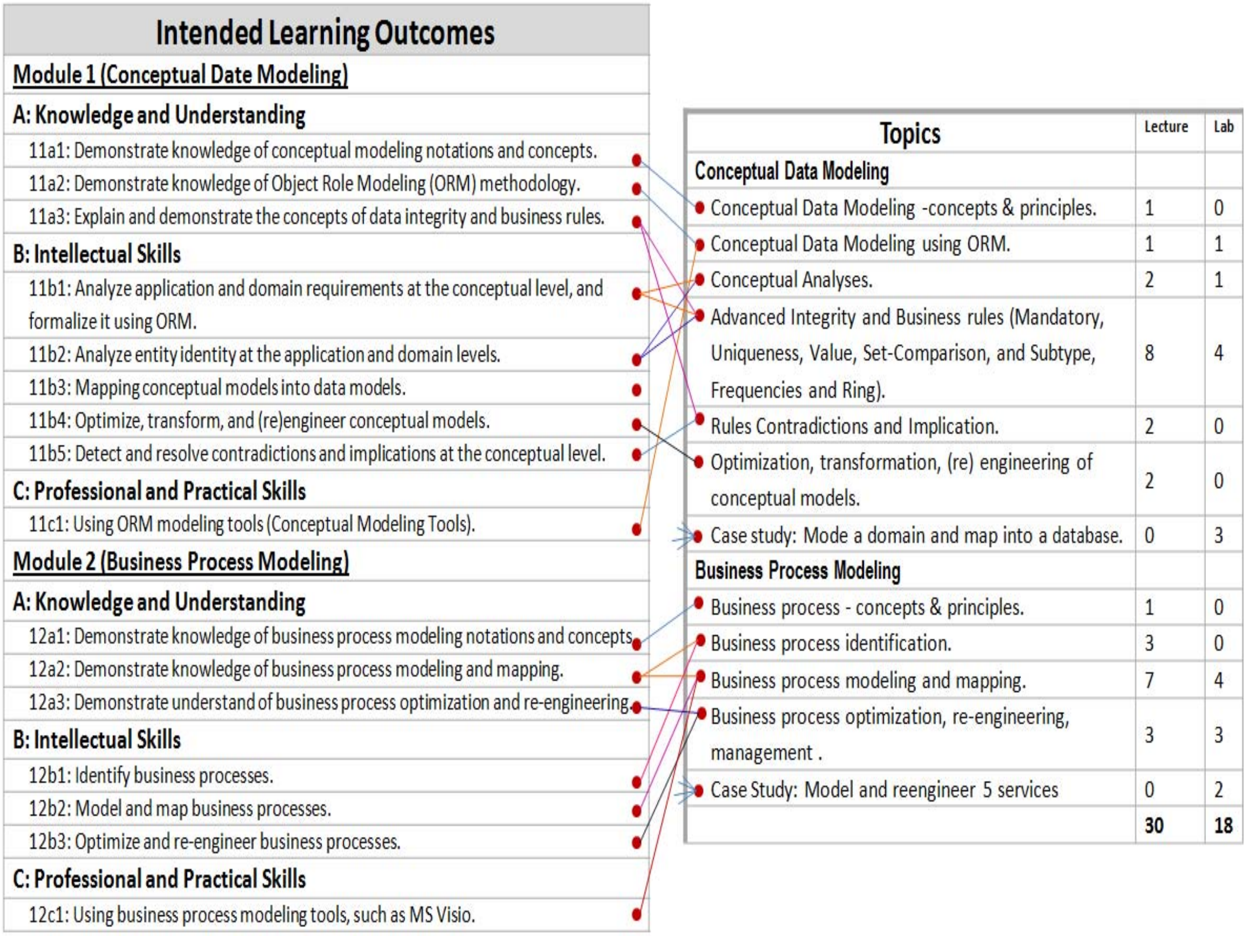
These tutorials are designed based on the needs assessment presented in the previous sections. That is, we analyzed the Palestinian e-Government Architecture and identified eight missing skills, presented in general terms. Each of these eight skills was then elaborated arriving at a set of more specific knowledge and skills that one needs in order to implement and deploy the e-Government Architecture. The set of specific missing skills can then be seen as the set of Intended Learning Objectives that our proposed tutorials aim to fulfill.

In addition, several meetings and interviews were conducted, among all Palestinian partner universities and ministries, to discuss and assess whether the identified needs and proposed topics were sound and comprehensive. The proposed topics and trainings in the six tutorials were also discussed with the EU partner universities, and compared with related courses there in order to assess the "up-to-date-ness" and integrity of the topics.


Process and Data Modeling
Information Security
Data Integration and open Information Systems
Process Integration and Service Oriented Architectures
Legal Informatics
Ontology Engineering and Lexical Semantics

4.1Tutorial 1: Process and Data Modeling

Prerequisites: Database, OO programming, and UML diagrams.

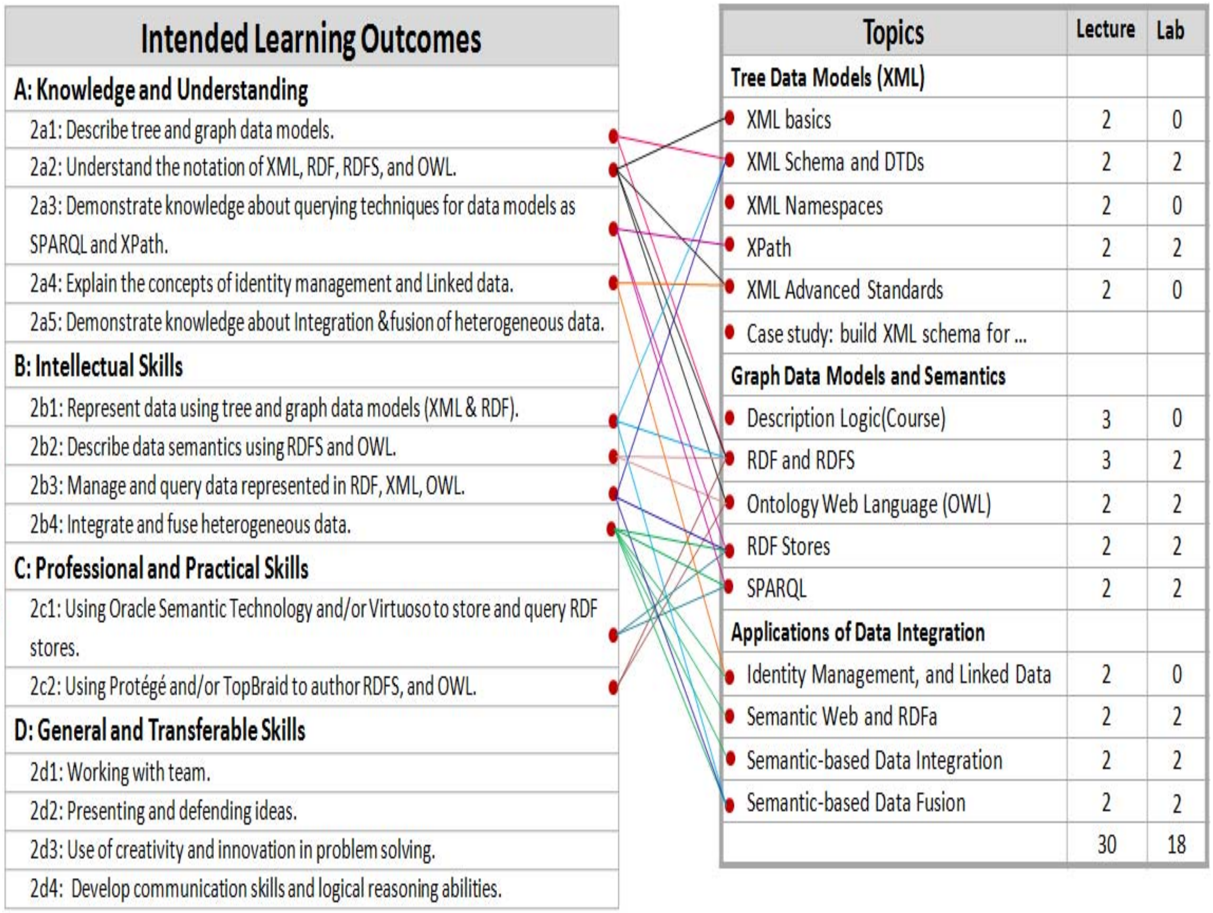


Intended Learning Outcomes
Module 1 (Conceptual Date Modeling)
A: Knowledge and Understanding
11a1: Demonstrate knowledge of conceptual modeling notations and concepts. ●
11a2: Demonstrate knowledge of Object Role Modeling (ORM) methodology. ●
11a3: Explain and demonstrate the concepts of data integrity and business rules. ●
B: Intellectual Skills
11b1: Analyze application and domain requirements at the conceptual level, and formalize it using ORM. ●
11b2: Analyze entity identity at the application and domain levels. ●
11b3: Mapping conceptual models into data models. ●
11b4: Optimize, transform, and (re)engineer conceptual models. ●
11b5: Detect and resolve contradictions and implications at the conceptual level. ●
C: Professional and Practical Skills
11c1: Using ORM modeling tools (Conceptual Modeling Tools). ●
Module 2 (Business Process Modeling)
A: Knowledge and Understanding
12a1: Demonstrate knowledge of business process modeling notations and concepts ●
12a2: Demonstrate knowledge of business process modeling and mapping. ●
12a3: Demonstrate understand of business process optimization and re-engineering ●
B: Intellectual Skills
12b1: Identify business processes. ●
12b2: Model and map business processes. ●
12b3: Optimize and re-engineer business processes. ●
C: Professional and Practical Skills
12c1: Using business process modeling tools, such as MS Visio. ●

Topics	Lecture	Lab
Conceptual Data Modeling		
● Conceptual Data Modeling -concepts & principles.	1	0
● Conceptual Data Modeling using ORM.	1	1
● Conceptual Analyses.	2	1
● Advanced Integrity and Business rules (Mandatory, Uniqueness, Value, Set-Comparison, and Subtype, Frequencies and Ring).	8	4
● Rules Contradictions and Implication.	2	0
● Optimization, transformation, (re) engineering of conceptual models.	2	0
● Case study: Mode a domain and map into a database.	0	3
Business Process Modeling		
● Business process - concepts & principles.	1	0
● Business process identification.	3	0
● Business process modeling and mapping.	7	4
● Business process optimization, re-engineering, management .	3	3
● Case Study: Model and reengineer 5 services	0	2
	30	**18**

4.2Tutorial 2: Data Integration and Open Information System

Prerequisites: Tutorial 1, HTML and web programming basics, First Order Logic

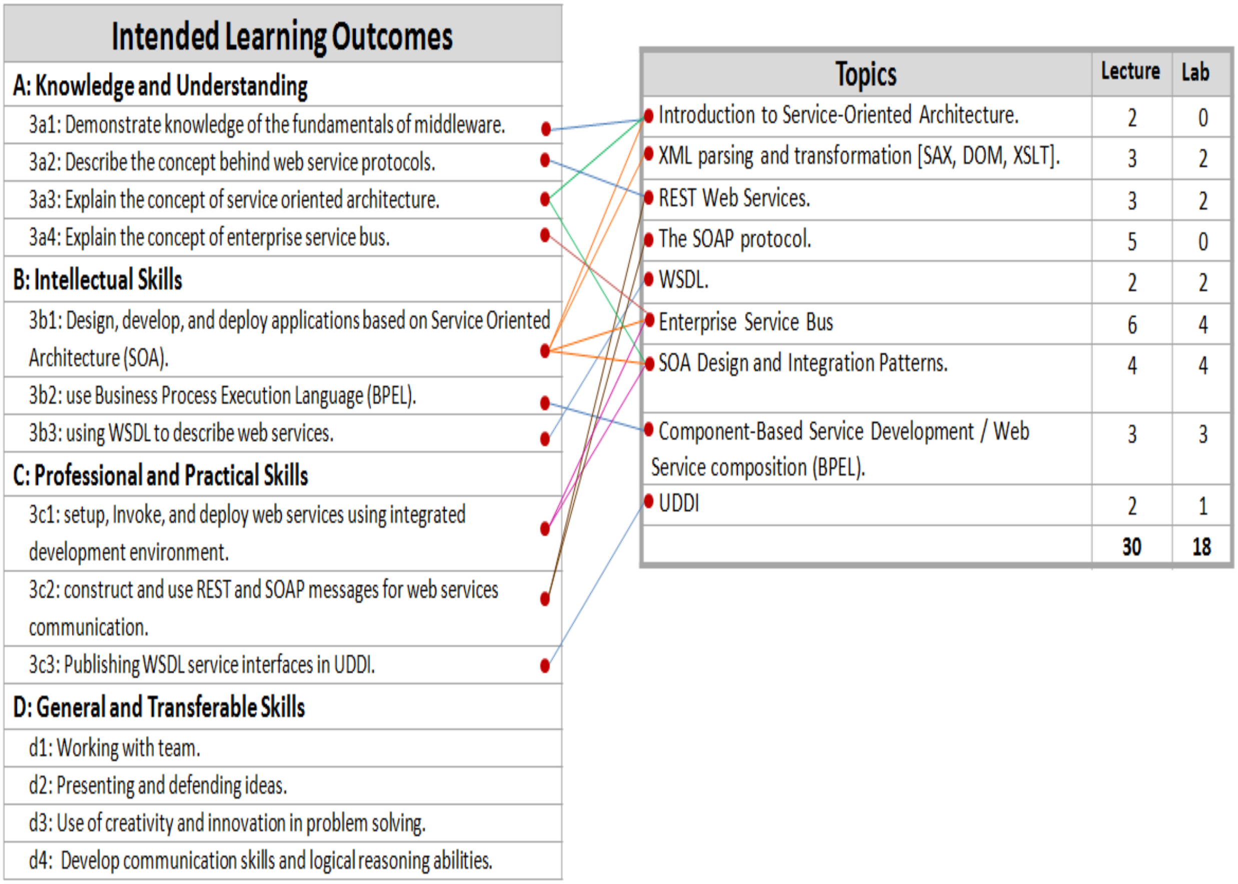


Intended Learning Outcomes
A: Knowledge and Understanding
2a1: Describe tree and graph data models.
2a2: Understand the notation of XML, RDF, RDFS, and OWL.
2a3: Demonstrate knowledge about querying techniques for data models as SPARQL and XPath.
2a4: Explain the concepts of identity management and Linked data.
2a5: Demonstrate knowledge about Integration &fusion of heterogeneous data.
B: Intellectual Skills
2b1: Represent data using tree and graph data models (XML & RDF).
2b2: Describe data semantics using RDFS and OWL.
2b3: Manage and query data represented in RDF, XML, OWL.
2b4: Integrate and fuse heterogeneous data.
C: Professional and Practical Skills
2c1: Using Oracle Semantic Technology and/or Virtuoso to store and query RDF stores.
2c2: Using Protégé and/or TopBraid to author RDFS, and OWL.
D: General and Transferable Skills
2d1: Working with team.
2d2: Presenting and defending ideas.
2d3: Use of creativity and innovation in problem solving.
2d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture	Lab
Tree Data Models (XML)		
● XML basics	2	0
● XML Schema and DTDs	2	2
● XML Namespaces	2	0
● XPath	2	2
● XML Advanced Standards	2	0
● Case study: build XML schema for …		
Graph Data Models and Semantics		
● Description Logic(Course)	3	0
● RDF and RDFS	3	2
● Ontology Web Language (OWL)	2	2
● RDF Stores	2	2
● SPARQL	2	2
Applications of Data Integration		
● Identity Management, and Linked Data	2	0
● Semantic Web and RDFa	2	2
● Semantic-based Data Integration	2	2
● Semantic-based Data Fusion	2	2
	30	18

4.3Tutorial 3: Process Integration and Service Oriented Architectures

Prerequisites: XML, XML Schema, OO programming and UML diagrams

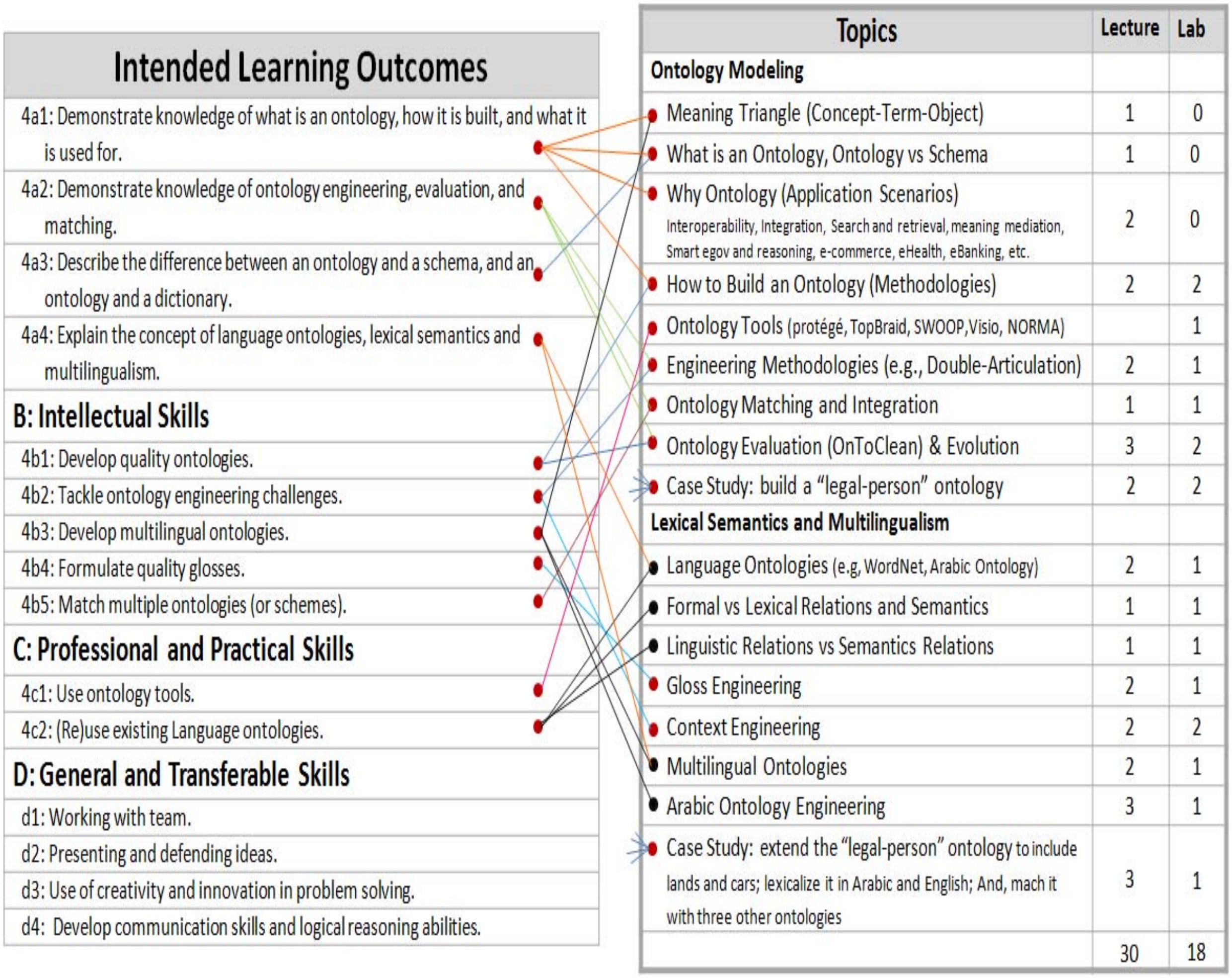


Intended Learning Outcomes
A: Knowledge and Understanding
3a1: Demonstrate knowledge of the fundamentals of middleware.
3a2: Describe the concept behind web service protocols.
3a3: Explain the concept of service oriented architecture.
3a4: Explain the concept of enterprise service bus.
B: Intellectual Skills
3b1: Design, develop, and deploy applications based on Service Oriented Architecture (SOA).
3b2: use Business Process Execution Language (BPEL).
3b3: using WSDL to describe web services.
C: Professional and Practical Skills
3c1: setup, Invoke, and deploy web services using integrated development environment.
3c2: construct and use REST and SOAP messages for web services communication.
3c3: Publishing WSDL service interfaces in UDDI.
D: General and Transferable Skills
d1: Working with team.
d2: Presenting and defending ideas.
d3: Use of creativity and innovation in problem solving.
d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture	Lab
Introduction to Service-Oriented Architecture.	2	0
XML parsing and transformation [SAX, DOM, XSLT].	3	2
REST Web Services.	3	2
The SOAP protocol.	5	0
WSDL.	2	2
Enterprise Service Bus	6	4
SOA Design and Integration Patterns.	4	4
Component-Based Service Development / Web Service composition (BPEL).	3	3
UDDI	2	1
	30	**18**

4.4Tutorial 4: Ontology Engineering and Lexical Semantics

Prerequisites: Tutorial-1, Tutorial-2



Intended Learning Outcomes
4a1: Demonstrate knowledge of what is an ontology, how it is built, and what it is used for.
4a2: Demonstrate knowledge of ontology engineering, evaluation, and matching.
4a3: Describe the difference between an ontology and a schema, and an ontology and a dictionary.
4a4: Explain the concept of language ontologies, lexical semantics and multilingualism.
B: Intellectual Skills
4b1: Develop quality ontologies.
4b2: Tackle ontology engineering challenges.
4b3: Develop multilingual ontologies.
4b4: Formulate quality glosses.
4b5: Match multiple ontologies (or schemes).
C: Professional and Practical Skills
4c1: Use ontology tools.
4c2: (Re)use existing Language ontologies.
D: General and Transferable Skills
d1: Working with team.
d2: Presenting and defending ideas.
d3: Use of creativity and innovation in problem solving.
d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture	Lab
Ontology Modeling		
Meaning Triangle (Concept-Term-Object)	1	0
What is an Ontology, Ontology vs Schema	1	0
Why Ontology (Application Scenarios) Interoperability, Integration, Search and retrieval, meaning mediation, Smart egov and reasoning, e-commerce, eHealth, eBanking, etc.	2	0
How to Build an Ontology (Methodologies)	2	2
Ontology Tools (protégé, TopBraid, SWOOP,Visio, NORMA)		1
Engineering Methodologies (e.g., Double-Articulation)	2	1
Ontology Matching and Integration	1	1
Ontology Evaluation (OnToClean) & Evolution	3	2
Case Study: build a "legal-person" ontology	2	2
Lexical Semantics and Multilingualism		
Language Ontologies (e.g, WordNet, Arabic Ontology)	2	1
Formal vs Lexical Relations and Semantics	1	1
Linguistic Relations vs Semantics Relations	1	1
Gloss Engineering	2	1
Context Engineering	2	2
Multilingual Ontologies	2	1
Arabic Ontology Engineering	3	1
Case Study: extend the "legal-person" ontology to include lands and cars; lexicalize it in Arabic and English; And, mach it with three other ontologies	3	1
	30	18

4.5Tutorial 5: Information Security

The basic objective is to cover the following competencies/Topics for government's technical employees. The first day session is for all employees, other days are for more technical staff with a degree in computing (Bsc.). This tutorial contains topics like Data Confidentiality, Data Integrity: Authenticity, Surreptitious forwarding, Non-repudiation, Access Control, Accounting and Logging and Availability related issues. Security Tutorial is 40 hours (23 hours theories and 17 practical hours)

Day 1		
Topics	**N. of Hours**	**ILO's**
Session 1 : Introduction • E-governments and security • Intro to security and threats (CIA) • ISO 27000 standards.	1 1 2	a1: a2: a3: b1: b2: b3 d3:
Session 2: Internet Risks and Attacks • Attacks on Internet Stack (routing, IP, DNS, UDP. • Symmetric and Asymmetric Cryptography. • DOS and DDOS	2 1 1	a1: a2 b1:b2:
Day 2		
Session 3: Authentication • Authentication (symmetric and asymmetric and 1 time password) • Introduction to LDAP	22	a2: b1: b3: b4: b5: d2: d3:
Session 4: Authentication Lab • Install apache and use basic authentication and hashed password files. (windows with administrative rights) • Install open LDAP • Apache with LDAP authentications	4	c1: c2: c3: c4: d1: d2:
Day 3		
Session 5: Certificates and Biometric Authentication • PKI and X.509 • SSL/TLS and IPSEC • Biometric authentication and smart cards.	1 1 2	b3: b4: b5: d2: d3:
Session 6: Certificates and Https Lab • Apache with LDAP authentications. • SSL practical (basic authentication over SSL, HTTPS) • Open SSL certificate and certificate authority	4	c1: c2: c3: c4: d1: d2:d3:

Day 4		
Session 7: Firewalls and VPN • Firewalls • VPNs • Secure DNS (or Secure wireless)	1 1 2	b3: b4:
Session 8: Firewalls and VPN and Biometric Lab • Fingerprints authentications • Firewall installations. • VPN installation.	1 1 2	c2: c3: c4: d1: d2:
Day 5		
Session 9: Firewalls and VPN and Biometric Lab • Federated Identity Management. • Privacy & Risk Management	2 2	a3: b1: b2: b3:b6: d3:
Session 9: FIM Lab • FIM LAB (TBA)	4	C5:

4.6Tutorial 6: The Legal Framework of New Technologies

This main objective of this tutorial is to provide governmental employees regardless of their specialization, with an understanding of legal application of new technologies concepts, data protection issues in e-government projects, ways of ensuring legal certainty and validity to e-government transactions, and coherence between e-government services.
Target: Government employees regardless to their specialization.

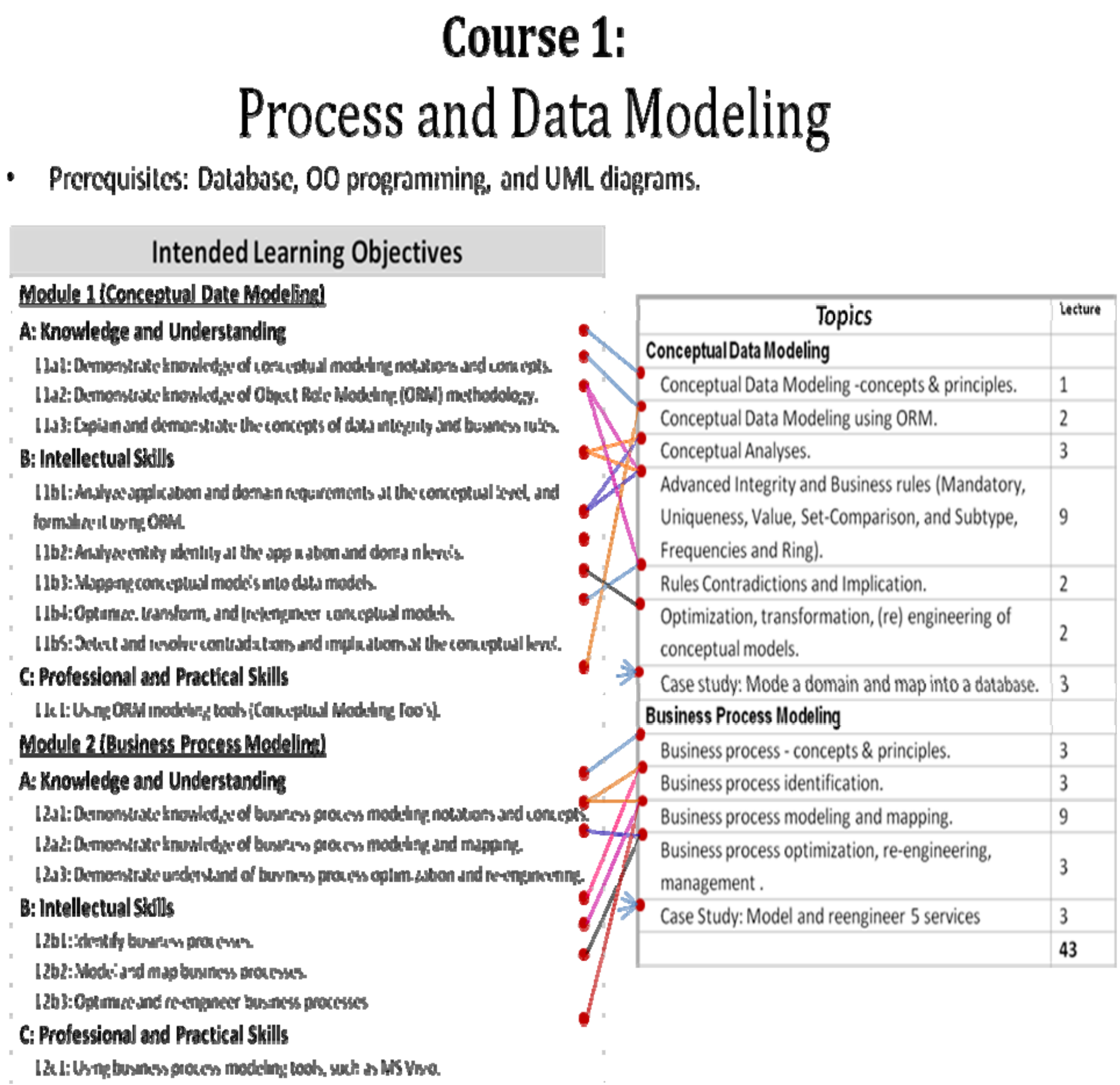
Topics	Hours	ILO's
Session1 : Introduction to Law • Evolution of the Palestinian Legal System • Public Law & international Law vs. Private Law	8	a1, a6, a8, a14
Session2: Ethical and Social Issues • Ethical and Social issues related to digital systems • Moral Dimensions of the Information Age • Responsibility, Accountability and Liability Candidate Ethical Principles	4	a1, a7, c1,c6, a14
Session3: Introduction to ICT and E-government • ICT concepts • E-government programmes and concept	8	a1,a2, a6, a14, d1, d3, d4
Session4: Intellectual Property • *Overview of Intellectual Property legislation in PNA* • *Trademark* • *Copyright* • *Patent*	3	A8, a14, c2, d1, d3, d4
Session 5: Privacy and Data Protection • Protecting Personal Privacy • Ensuring confidentiality • Implementing Appropriate Security Controls	7	a1, a2, a9, a14, b1, c1, d1, d3, d4
Session 6: Digital Signature & e-evidence • Legal framework of e-evidence in the PNA • Digital signature definition (IT Concept) • Regulating Digital signature in Palestine	5	A3, a9, a4, a14, c1, c5, b2, d1, d3, d4
Session 7: E-Commerce (e-transactions) • Legal framework relating to e-commerce in the PNA. (3) • Electronic Commerce Fundamentals • Electronic Transaction Models	3	A1, a10, a 14,c4, d1, d3, d4
Session 7: e-contract (IT contract) • E-contract definition	3	A1, a11, d1, d3, d4

• Application of IT contract		
Session 8: Cybercrime • General introduction to Cybercrime • Nature and scope of cybercrime • Example of cybercrime.	3	A1, a12, a14, b2, c1, d1, d3, d4
Session 9: E-archiving • Legal requirements of e-archiving • Automation, application and e-archiving	2	A13, a14, d1, d3, d4
Session 10: Case studies: e-ID, e-Passport & e-justice	4	A, b, c, d1,d2, d3, d4
Session 11: Discussion papers: Any topic of the above mentioned sessions	4	B, d1,d2, d3, d4
Total Hours	54	

5. The Proposed Academic Courses

Interoperability courses:
The following four Interoperability courses will be offered for fourth year IT bachelor degree and master degree students. Lectures will be the main delivery methodology, home work and case study also will be used, papers reading must be considered as part of the homework. Labs will be opened for students. Detailed syllabus will be developed for each course depending on the ILOs and the main topics.

5.1Course1: Process and Data Modeling



Course 1:
Process and Data Modeling

- Prerequisites: Database, OO programming, and UML diagrams.

Intended Learning Objectives

Module 1 (Conceptual Date Modeling)

A: Knowledge and Understanding

I1a1: Demonstrate knowledge of conceptual modeling notations and concepts.
I1a2: Demonstrate knowledge of Object Role Modeling (ORM) methodology.
I1a3: Explain and demonstrate the concepts of data integrity and business rules.

B: Intellectual Skills

I1b1: Analyze application and domain requirements at the conceptual level, and formalize it using ORM.
I1b2: Analyze entity identity at the application and domain levels.
I1b3: Mapping conceptual models into data models.
I1b4: Optimize, transform, and (re)engineer conceptual models.
I1b5: Detect and resolve contradictions and implications at the conceptual level.

C: Professional and Practical Skills

I1c1: Using ORM modeling tools (Conceptual Modeling Tools).

Module 2 (Business Process Modeling)

A: Knowledge and Understanding

I2a1: Demonstrate knowledge of business process modeling notations and concepts.
I2a2: Demonstrate knowledge of business process modeling and mapping.
I2a3: Demonstrate understand of business process optimization and re-engineering.

B: Intellectual Skills

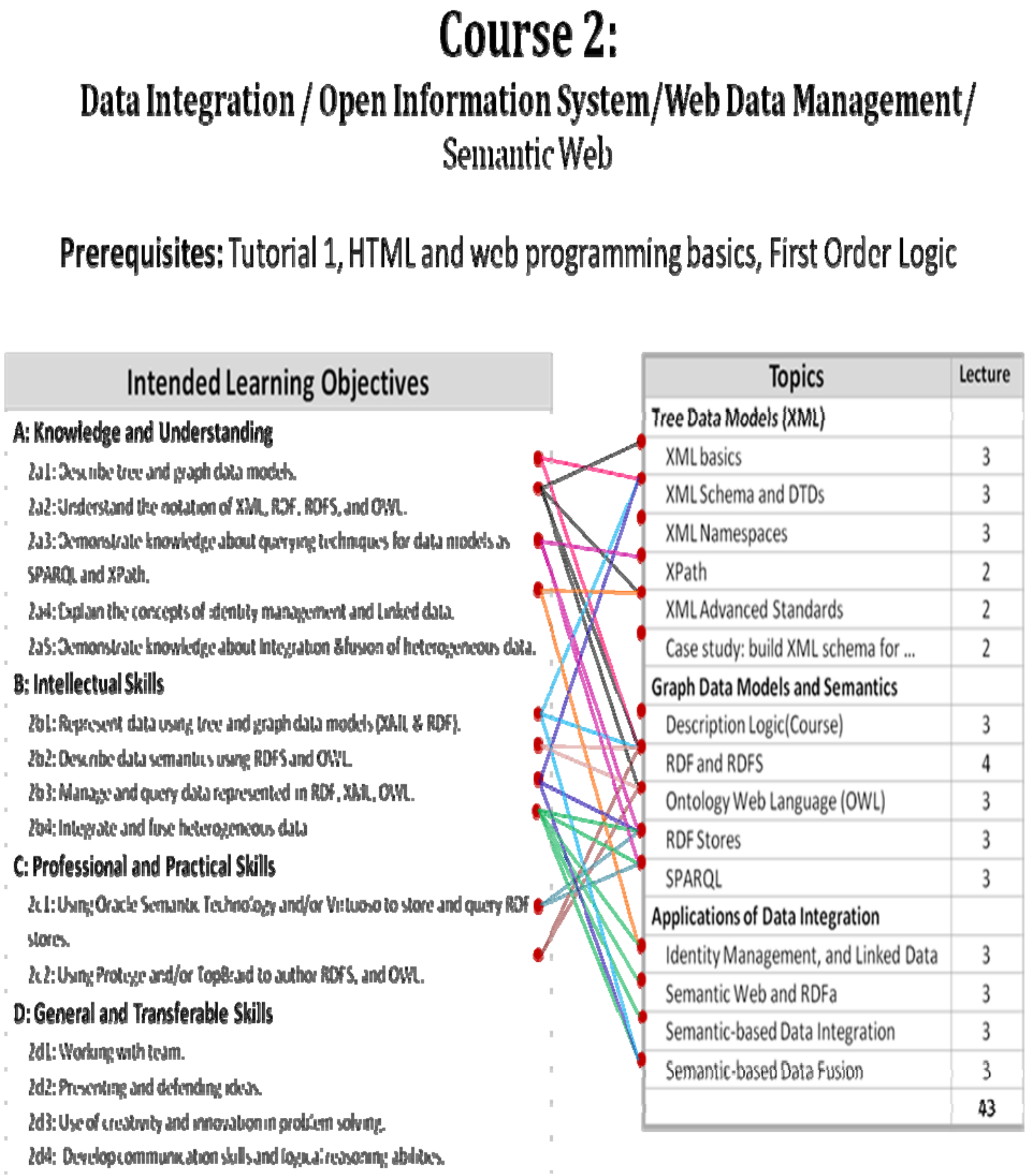
I2b1: Identify business processes.
I2b2: Model and map business processes.
I2b3: Optimize and re-engineer business processes

C: Professional and Practical Skills

I2c1: Using business process modeling tools, such as MS Visio.

Topics	Lecture
Conceptual Data Modeling	
Conceptual Data Modeling -concepts & principles.	1
Conceptual Data Modeling using ORM.	2
Conceptual Analyses.	3
Advanced Integrity and Business rules (Mandatory, Uniqueness, Value, Set-Comparison, and Subtype, Frequencies and Ring).	9
Rules Contradictions and Implication.	2
Optimization, transformation, (re) engineering of conceptual models.	2
Case study: Mode a domain and map into a database.	3
Business Process Modeling	
Business process - concepts & principles.	3
Business process identification.	3
Business process modeling and mapping.	9
Business process optimization, re-engineering, management .	3
Case Study: Model and reengineer 5 services	3
	43

5.2Course2: Data Integration



Course 2:

Data Integration / Open Information System/Web Data Management/ Semantic Web

Prerequisites: Tutorial 1, HTML and web programming basics, First Order Logic

Intended Learning Objectives

A: Knowledge and Understanding

2a1: Describe tree and graph data models.

2a2: Understand the notation of XML, RDF, RDFS, and OWL.

2a3: Demonstrate knowledge about querying techniques for data models as SPARQL and XPath.

2a4: Explain the concepts of identity management and Linked data.

2a5: Demonstrate knowledge about Integration &fusion of heterogeneous data.

B: Intellectual Skills

2b1: Represent data using tree and graph data models (XML & RDF).

2b2: Describe data semantics using RDFS and OWL.

2b3: Manage and query data represented in RDF, XML, OWL.

2b4: Integrate and fuse heterogeneous data

C: Professional and Practical Skills

2c1: Using Oracle Semantic Technology and/or Virtuoso to store and query RDF stores.

2c2: Using Protege and/or TopBraid to author RDFS, and OWL.

D: General and Transferable Skills

2d1: Working with team.

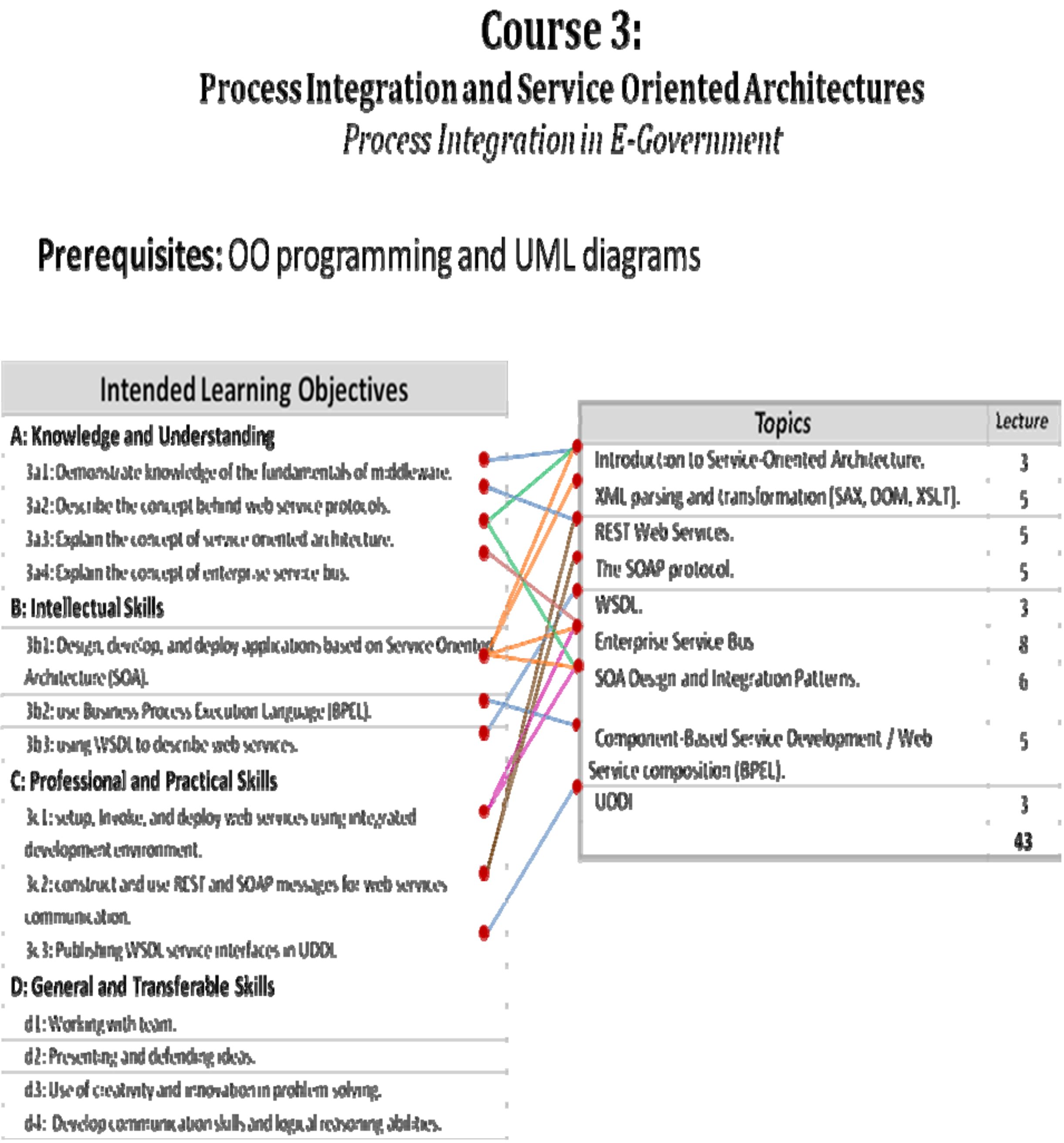
2d2: Presenting and defending ideas.

2d3: Use of creativity and innovation in problem solving.

2d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture
Tree Data Models (XML)	
XML basics	3
XML Schema and DTDs	3
XML Namespaces	3
XPath	2
XML Advanced Standards	2
Case study: build XML schema for ...	2
Graph Data Models and Semantics	
Description Logic(Course)	3
RDF and RDFS	4
Ontology Web Language (OWL)	3
RDF Stores	3
SPARQL	3
Applications of Data Integration	
Identity Management, and Linked Data	3
Semantic Web and RDFa	3
Semantic-based Data Integration	3
Semantic-based Data Fusion	3
	43

5.3Course3: Process Integration and Service Oriented Architectures



Course 3:

Process Integration and Service Oriented Architectures

Process Integration in E-Government

Prerequisites: OO programming and UML diagrams

Intended Learning Objectives

A: Knowledge and Understanding

3a1: Demonstrate knowledge of the fundamentals of middleware.

3a2: Describe the concept behind web service protocols.

3a3: Explain the concept of service oriented architecture.

3a4: Explain the concept of enterprise service bus.

B: Intellectual Skills

3b1: Design, develop, and deploy applications based on Service Oriented Architecture (SOA).

3b2: use Business Process Execution Language (BPEL).

3b3: using WSDL to describe web services.

C: Professional and Practical Skills

3c1: setup, Invoke, and deploy web services using integrated development environment.

3c2: construct and use REST and SOAP messages for web services communication.

3c3: Publishing WSDL service interfaces in UDDI.

D: General and Transferable Skills

d1: Working with team.

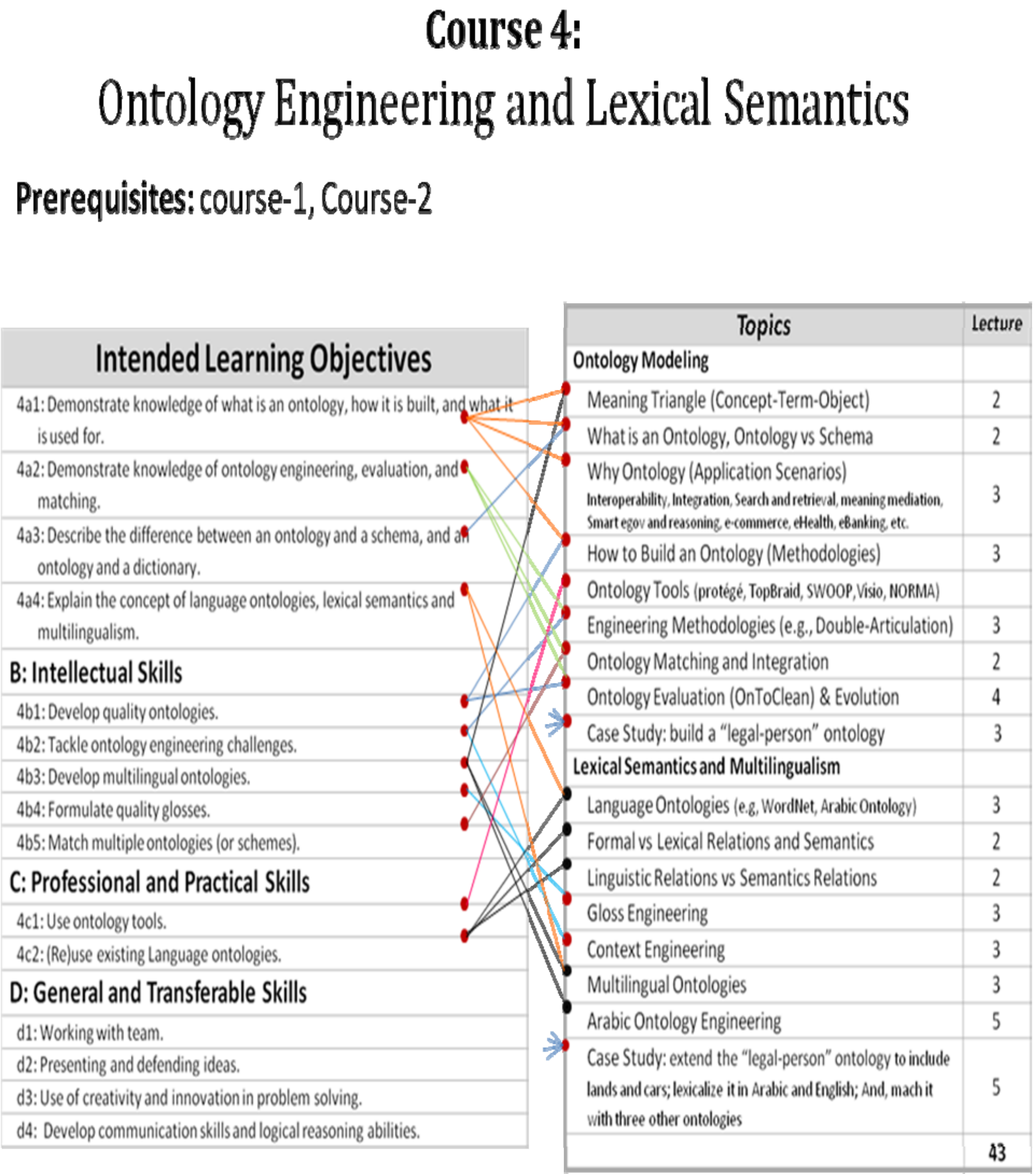
d2: Presenting and defending ideas.

d3: Use of creativity and innovation in problem solving.

d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture
Introduction to Service-Oriented Architecture.	3
XML parsing and transformation (SAX, DOM, XSLT).	5
REST Web Services.	5
The SOAP protocol.	5
WSDL.	3
Enterprise Service Bus	8
SOA Design and Integration Patterns.	6
Component-Based Service Development / Web Service composition (BPEL).	5
UDDI	3
	43

5.4Course4: Ontology Engineering and Lexical Semantics



Course 4:
Ontology Engineering and Lexical Semantics

Prerequisites: course-1, Course-2

Intended Learning Objectives
4a1: Demonstrate knowledge of what is an ontology, how it is built, and what it is used for.
4a2: Demonstrate knowledge of ontology engineering, evaluation, and matching.
4a3: Describe the difference between an ontology and a schema, and an ontology and a dictionary.
4a4: Explain the concept of language ontologies, lexical semantics and multilingualism.
B: Intellectual Skills
4b1: Develop quality ontologies.
4b2: Tackle ontology engineering challenges.
4b3: Develop multilingual ontologies.
4b4: Formulate quality glosses.
4b5: Match multiple ontologies (or schemes).
C: Professional and Practical Skills
4c1: Use ontology tools.
4c2: (Re)use existing Language ontologies.
D: General and Transferable Skills
d1: Working with team.
d2: Presenting and defending ideas.
d3: Use of creativity and innovation in problem solving.
d4: Develop communication skills and logical reasoning abilities.

Topics	Lecture
Ontology Modeling	
Meaning Triangle (Concept-Term-Object)	2
What is an Ontology, Ontology vs Schema	2
Why Ontology (Application Scenarios) Interoperability, Integration, Search and retrieval, meaning mediation, Smart egov and reasoning, e-commerce, eHealth, eBanking, etc.	3
How to Build an Ontology (Methodologies)	3
Ontology Tools (protégé, TopBraid, SWOOP, Visio, NORMA)	
Engineering Methodologies (e.g., Double-Articulation)	3
Ontology Matching and Integration	2
Ontology Evaluation (OnToClean) & Evolution	4
Case Study: build a "legal-person" ontology	3
Lexical Semantics and Multilingualism	
Language Ontologies (e.g, WordNet, Arabic Ontology)	3
Formal vs Lexical Relations and Semantics	2
Linguistic Relations vs Semantics Relations	2
Gloss Engineering	3
Context Engineering	3
Multilingual Ontologies	3
Arabic Ontology Engineering	5
Case Study: extend the "legal-person" ontology to include lands and cars; lexicalize it in Arabic and English; And, mach it with three other ontologies	5
	43

5.5 Course5: Information Security

The basic objective is to cover the following competencies/Topics for university students. The course can be a 4th year course or as special topics course for undergraduate students. Students should have basic or introductory course in Networking. This course contains topics like Data Confidentiality, Data Integrity: Authenticity, Surreptitious forwarding, Non-repudiation, Access Control, Accounting and Logging and Availability related issues. Security course is a standard 48 hours that can be registered as a 3 credit hours course.

Security Course Learning Objectives

a) Understand the importance of taking a systems wide approach to maintaining information security, and the balance between risk and expenditure.
b) Have an understanding of the threats faced by computer operating systems, applications and networks (especially the Internet) and the various countermeasures that can be used;
c) Have a basic understanding of the algorithms used in cryptography;
d) Understand the motivation, design, operation and management of modern systems for encryption, authentication, authorization and identification.
e) Have an understanding of the various techniques used in identity management;
f) The ability to analyze the information security requirements of an organization.
g) Skills to use the appropriate software tools, techniques and packages to produce and develop security systems especially in the area of authentication.
h) Be able to make informed choices of the appropriate security measures to put into place for a given network, operating system or application;
i) Be able to undertake practical exercises related to securing computer systems;

ILOs

A: Knowledge and Understanding

a1: Define the different risks and threats from being connected to networks, internet and web applications.

a2: Defines security standards and policies.

a3: Recognize risk assessment and management

B: Intellectual Skills

b1: Illustrate the different risks and threats from being connected.

b2: Relates risk assessment and management to e-government model.

b3: Design end-to-end secure and available systems.

b4: design integral and confidentiality services.

b5: design user authentication and authorization services.

b6: develop security policies.

C: Professional and Practical Skills

c1: Deploy and configure a secure system to protect their computing resources.

c2: Configure an end-to-end secure and available system using Apache.

c3: Configure integral and confidentiality services using integrity and confidentiality algorithms and protocols.

c4: Configure user authentication and authorization services using LDAP and SSL certificates.

c5: Implement a federated Identity Management to e-government model (??).

D: General and Transferable Skills

d1: Communication and team work.

d2: Systems configurations.

d3: Analysis and identification skills.

Topics	**Weeks/Hours**
Introduction to Computer / Network / Information Security.	1.5
Attacks on the Internet protocols	1.5
Introduction to cryptography (symmetric and asymmetric, and HMAC)	3
Authentication using Symmetric Techniques, KERBOROS, One Time Passwords and Scratch Cards, Schneider, MAX	3
Authentication using Symmetric Techniques PKI and X.509 , PGP.	3
SSL/TLS/VPN	3
Biometric Authentication	1.5
First Exam	**1.5**
Smart Cards	1.5
Authorizations (DAC, MAC, and RBACK)	3
Policy Based Authorizations PDPs, PEP	3
Intrusion Detect	1.5
DOS, DDOS	1.5
Malicious Software	1.5
Second Exam	**1.5**
Firewalls, IDS, IPS	1.5
IPSEC	1.5
Secure DNS	1.5
Secure Wireless	3
Security Management and ISO 27000	3
Review & Final Exams	

Teaching Methods:

Methods
Lecture
Reading
Independent work
Group work
Projects
Discussions

5.6Course6: Legal Framework of New Technologies

This main objective of this course is to provide students with an understanding of the Legal Framework of New Technologies concepts, data protection issues in e-government projects, ways of ensuring legal certainty and validity to e-government transactions, and coherence between e-government services.
Target: Informatics students.
Pre-requisites: Introduction to information systems, Information Security, Interoperability.

Legal Framework of New Technologies Objectives

a) Understanding data protection issues in an e-government project
b) Ensuring legal certainty and validity to e-government transactions
c) Ensuring coherence between e-government services

A: Knowledge and Understanding:

a:1 understand the legal frame for access management
a2: Enforcing security management through internal regulation
a3: Understanding the current non electronic evidence law
a4: Understanding the legal framework for digital signature, certificate and third party certification
a5: Understanding the general framework for e-government transfer of information
a6: Understand the importance of policy making in the legislative process
a7:Inhance knowledge on ethics related to digital systems
a8: Wide the awareness of students & lawyers to the best practices related to IP laws & applications
a9: Widen the knowledge of privacy and data protection
a10 Enhance general understandings of e-commerce
a11: Enhance knowledge of e-contract
a.12: Enhance and understand Cybercrime
a.13 Understanding of e-archiving
a.14: Develop knowledge about international as well as EU best practices and standards

B: Intellectual Skills:

b1: Ensure public transparency of the processing of data.
b2: Ensure the workability of a e-government service

C: Professional and Practical Skills:

c1: Control of the processing of personal data by public bodies.
c2: Ensuring international transfer of data
c3: Ensuring validity of e-signature
c4: Assessing the legal admissibility of an electronic document
c5: Assessing the need for a digital signature
c6: Managing the relationship between the citizens and the public bodies in charges of e-services?

D: Transferable Skills:

d1: Team Work.
d2: Governmental legal issues.
d3: Analysis skills
d4: Research paper

Course Outline and Calendar:

Seq.	Topics	**Hours**
1.	Introduction to the Science of Law	**3**
2.	Social and political aspects	3
3.	Ethical and Social Issues	3
4.	E-Government and Individual Privacy	3
5.	Government Data Privacy	3
6.	First Exam	1.5
7.	The Legal Framework for e-Government	6
8.	An evaluation framework for e-government projects	3
9.	Comparing Citizens' Use of E-Government to Alternative Service Channel	3
10.	Evaluating the Impact of E-government on Citizens	3
11.	Second Exam	1.5
12.	Considering the Role of E-government in Cybercrime Awareness and Prevention	3
13.	Assessing e-Government Services	3
14.	Electronic Surveillance	3
15.	Final Exam	3

Teaching Methods:

Methods
Lecture
Reading
Independent work
Group work
Projects
Discussions

6. References

[1] http://www.mtit.pna.ps

[2] http://www.w3.org/TR/ws-arch/

[3] http://www.w3.org/TR/soap/

[4] http://www.w3.org/TR/wsdl

[5] http://zinnar.pna.ps

[6] http://en.wikipedia.org/wiki/Data_integration

[7] http://en.wikipedia.org/wiki/Data_fusion

[8] Ministry of Telecommunication and Information Technology: e-Government Program, *Palestine X-Road: Palestinian e-Government Architecture*. Ramallah, Palestine. January 2011.

[9] Ministry of Telecommunication and Information Technology: e-Government Program, *Palestinian Interoperability Framework (Technical Report).* Ramallah, Palestine. November 2010.