TRUSTED VISION

Data Classification Proposals

Version 1.0

Date: 24-November-2025

Contact Information

For inquiries about this document and the information received, you can contact the people listed on the table below:

Name	**Hashem Al Azizi**
Phone Number	**+966-53-122-1580**
Email	**Hashem.azizi@trustedvision.biz**
Address	**Qurtuba District Saeed Bin Zaid Street** **P.O. Box 13247, Building No. 6482** **Riyadh - Kingdom of Saudi Arabia**

TRUSTED VISION

Table of Contents

1. Executive Summary

Trusted Vision is delighted to offer consulting services in the development and implementation of data classification to Marna.

1.2 Data Classification Consultation Services Overview

Data Classification domain is recognized as number 13 in the Data Management and Personal Data Protection Framework (Figure 1). This project is aimed at establishing a unified framework that categorizes data into distinct levels, defines mechanisms for handling it, and assesses the impact severity stemming from unauthorized data disclosure or access to its content.

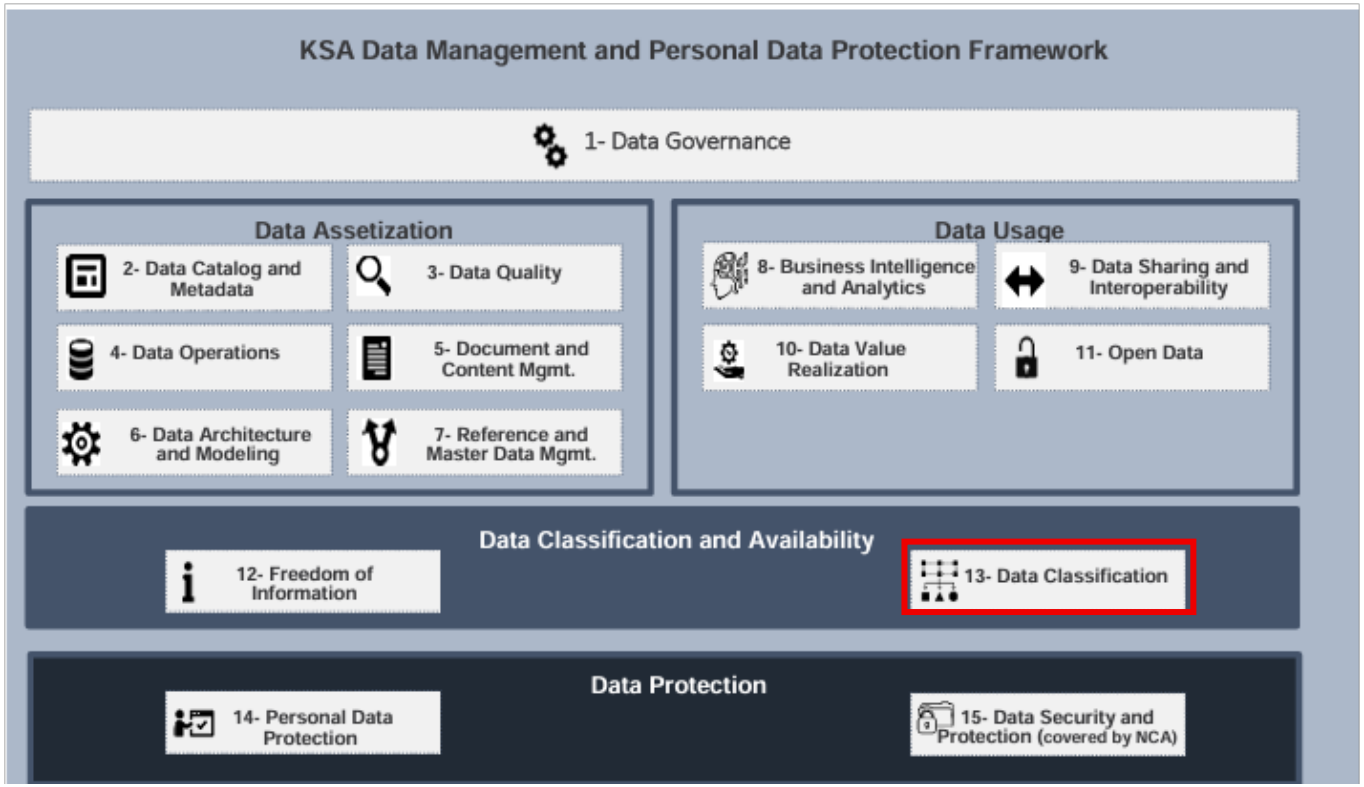


Figure 1 KSA Data Management and Personal Data Protection Framework

We believe that our experience in implementing similar projects positions us among the elite consulting firms, in addition to:

1. A balanced blend of international and local expertise in cybersecurity.
2. An effective approach to project implementation that ensures project requirements are met timely, professionally, and with high quality.
3. Extensive knowledge and experience in implementing and designing solutions based on international standards and best practices.
4. Premier cybersecurity consulting expertise.

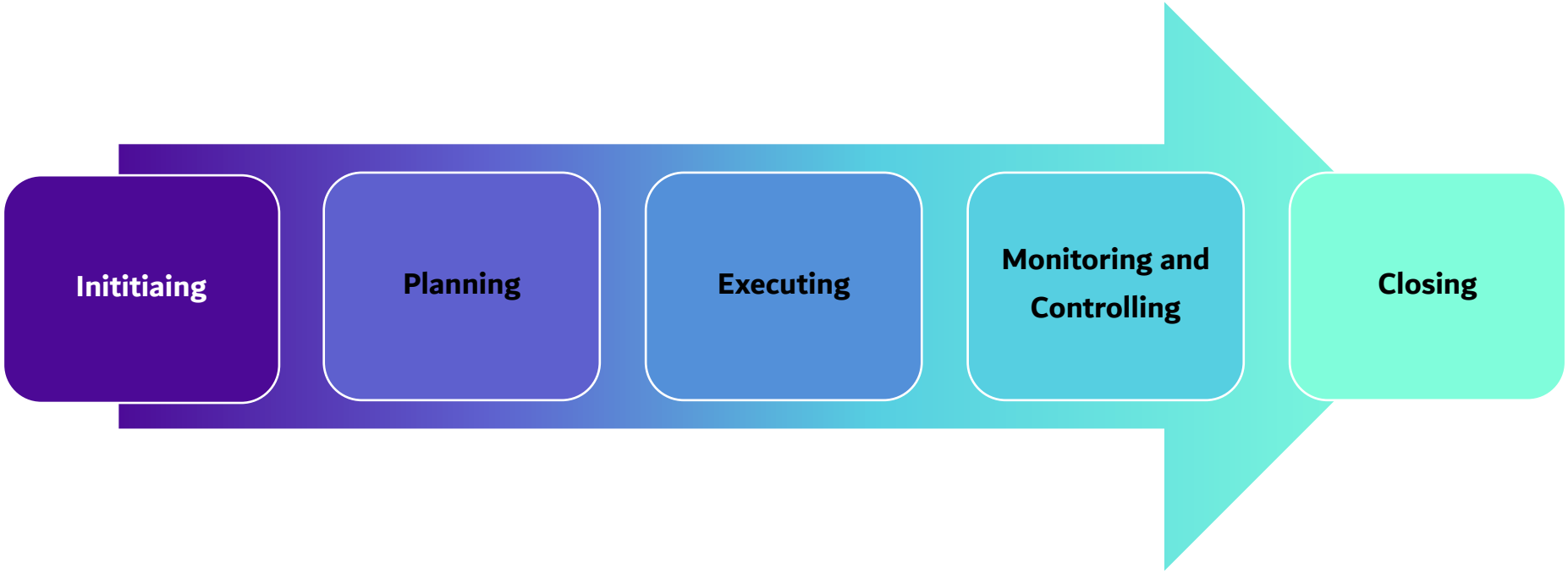
We hope that our consulting services meet the competitive requirements and look forward to establishing a mutually beneficial working relationship.

2. Project Benefits

The implementation of this project will provide the entity with the following benefits:

1. Compliance with Domain 13 of the National Data Management, Governance, and Personal Data Protection Framework (NDMO)
2. Data classification serves as the foundational pillar for the implementation of data security controls issued by the National Cybersecurity Authority (NCA-DCC).
3. Accurate data classification enhances the effectiveness of data management, leading to cost reductions related to the storage, processing, and maintenance of data.
4. Fosters a culture that recognizes the importance and sensitivity of data, enhancing overall organizational awareness and responsiveness.
5. Minimizes the risks and costs associated with data breaches and cybersecurity threats, safeguarding organizational assets and reputation.
6. Manages the assurance, integrity, security, value, and availability of data.
7. Increased customer and interested party satisfaction.
8. Reduced costs because of data breaches

3. Project Management and Implementation Methodology

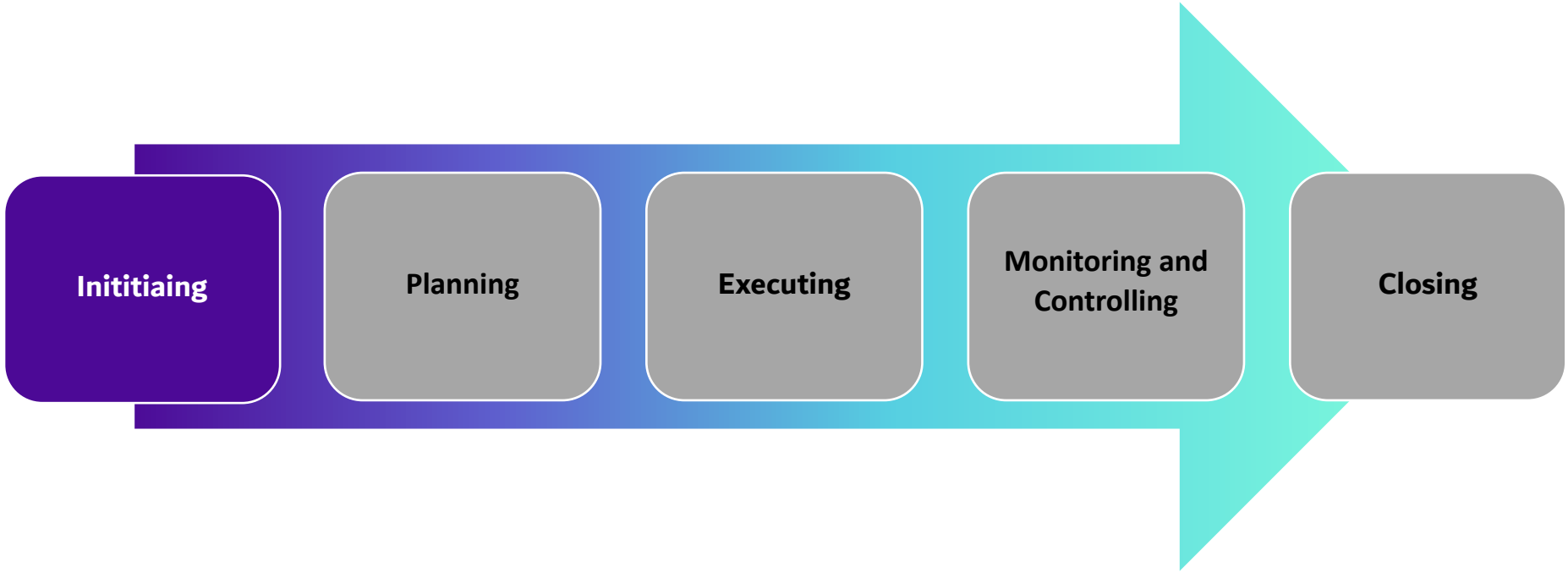


At Trusted Vision, we adhere to the PMI's global project management methodology, which encompasses initiating, planning, executing, monitoring and controlling, and closing phases.

Note: The cooperation of the entity and its employees is crucial, sensitive, and necessary to ensure the success of this project.

Note: Some documents may be consolidated and delivered as a single document as needed, according to the requirements and circumstances of the entity.

3.1. Initiation Phase



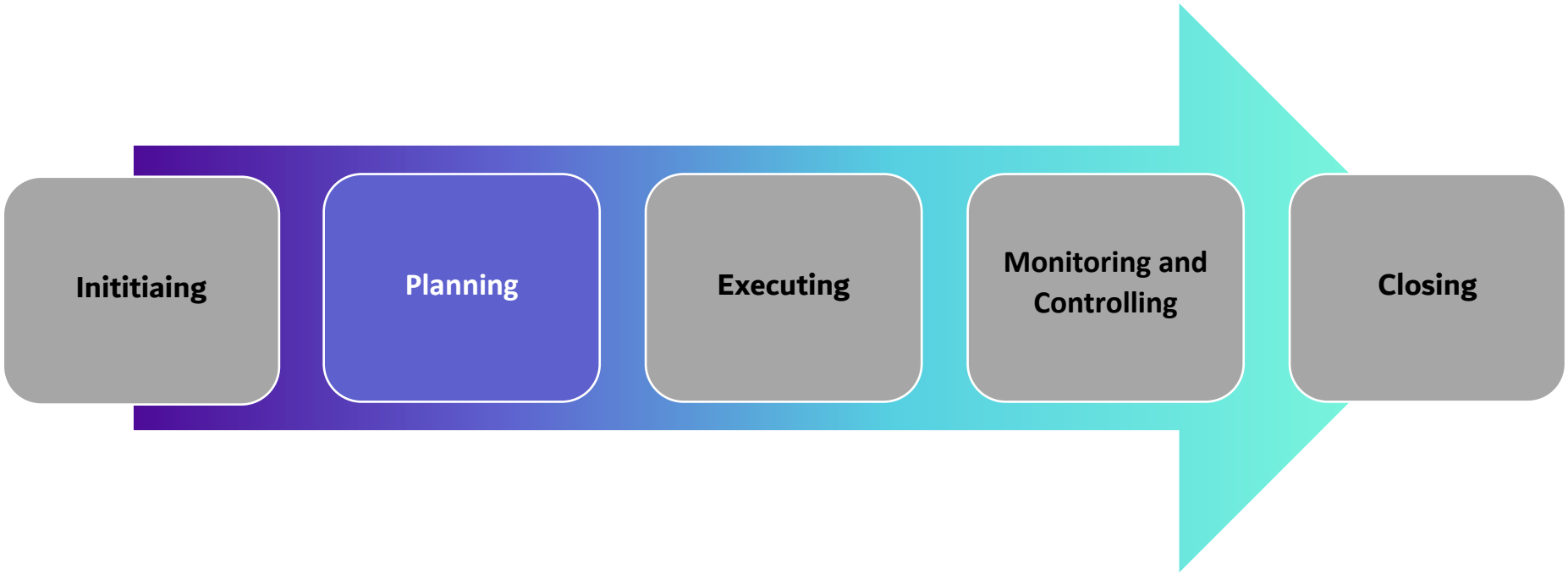
At this stage, the project is defined, and the project leader identifies their authority, the key stakeholders, the most significant anticipated risks, and the critical deliveries. All these elements are documented in the project charter.

The table below lists the activities that will be conducted during this stage:

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Proposed Timeline	Completed activities and materials delivered to the entity
I-1	Mobilizing the project team	Allocating a project manager from the entity to work with consultants	1 Day	A team equipped to start the project

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Proposed Timeline	Completed activities and materials delivered to the entity
I-2	Identify stakeholders	-	-	Identify stakeholders
I-3	Project Charter Development	Review and approve the project charter	3 Days	Project Charter Document
I-4	Perform Kick-off meeting with main interested people	Coordinate the Kick-off meeting and ensure all stakeholders attendance	1 Day	Kick-off meeting with main interested people with meeting minutes

3.2. Planning Phase



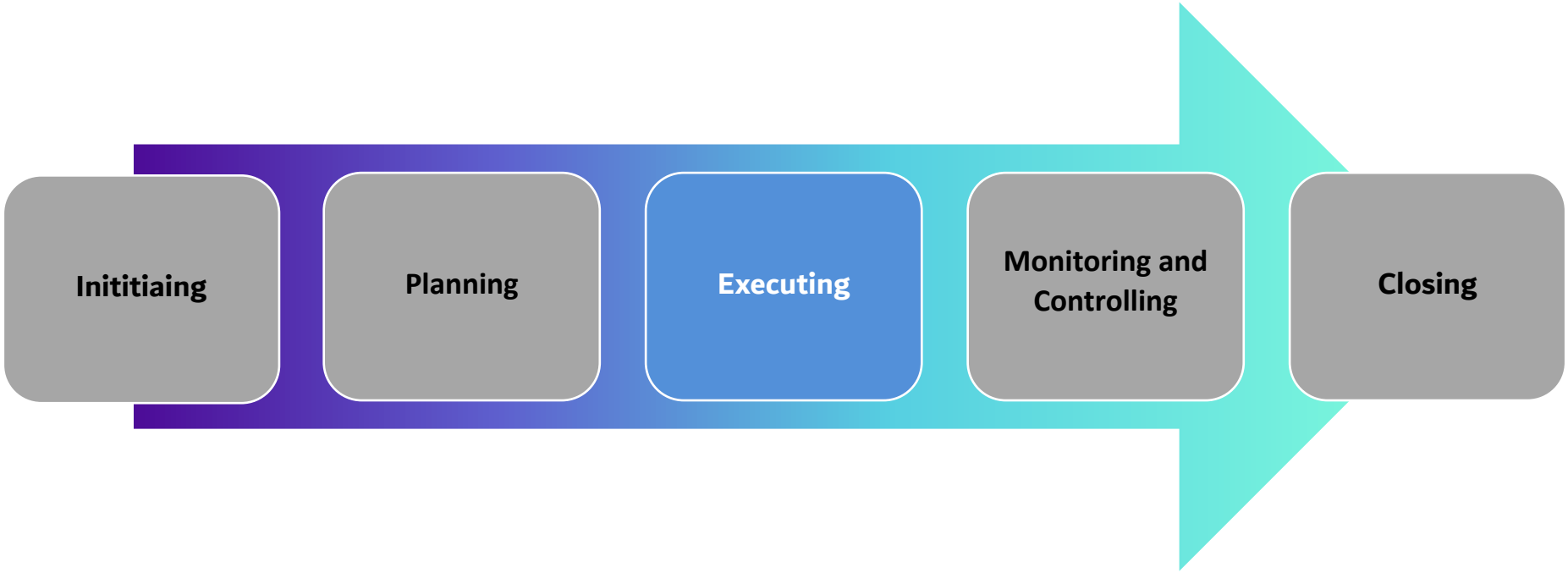
At this stage, the scope is defined and limited, methods of work are determined to achieve the goals.

The table below outlines the activities that will be conducted during this stage:

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
P-1	Collection and inventory of information security policies, procedures, processes and forms, which include 1. Policies & Procedures	Send all required documents and information	5 days	Meeting Minutes

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
	2. KPIs and KRIs 3. Key risk indicators 4. Current Risk management Framework 5. Cybersecurity Procedures and Forms 6. Cybersecurity Risk register 7. Inventory for the systems in the scope of the assessment. 8. Roles and Responsibilities			
P-2	Conducting interviews with departments and related parties: • Cybersecurity Department • Information Technology Department • Cyber Security Management • Customer Care Management • Marketing Management • Interview with other departments	Coordinate interview	5 days	Minutes of meetings
P-3	Understand all data assets, environment, and current data classification challenges.	Send all required information and documents	-	-

1.3 Executing Phase



At this stage, the project is executed according to the predefined plan to achieve the expected outputs.

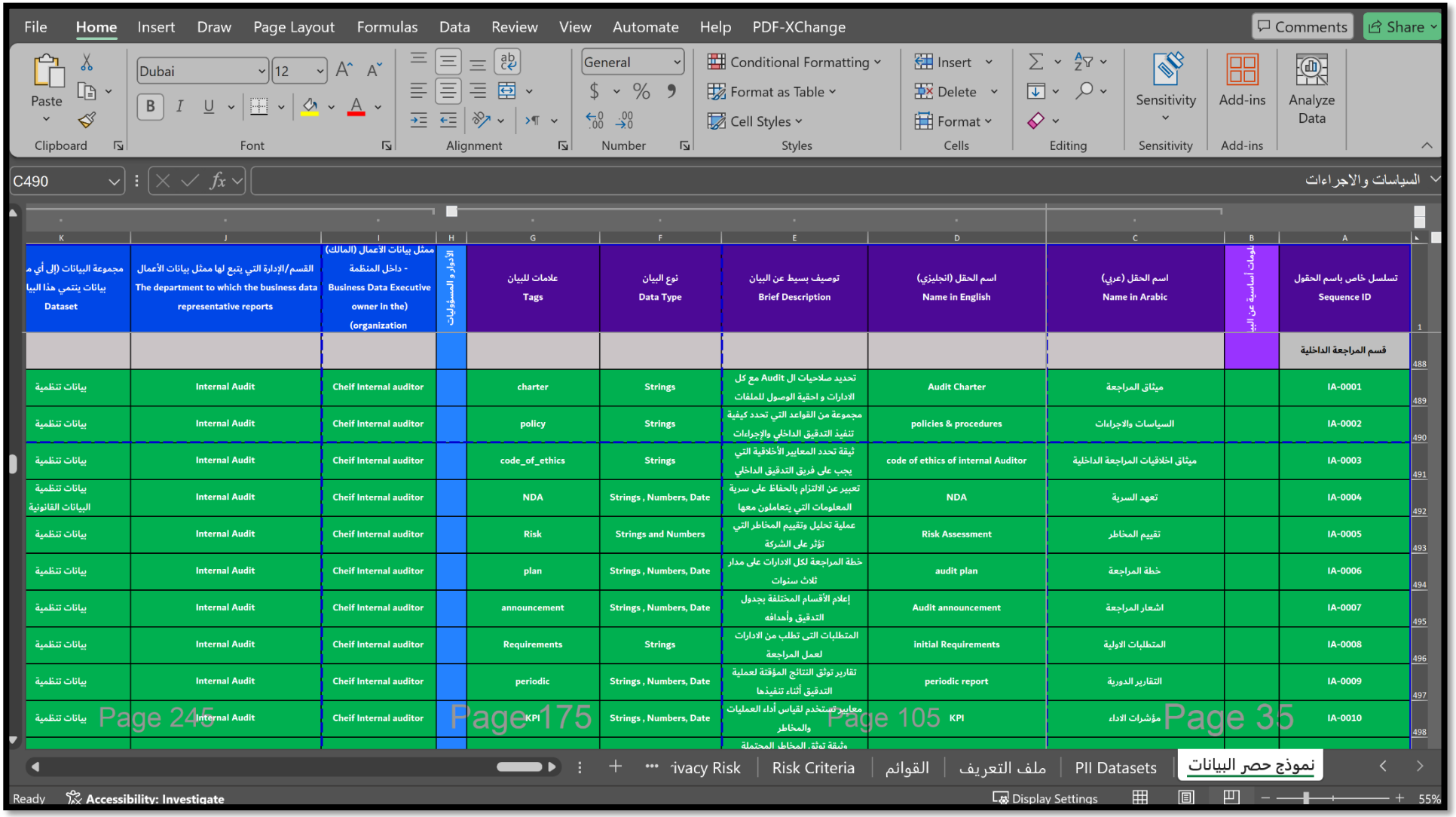
The table below contains the activities that will be carried out at this stage:

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
E-1	Develop data classification policy and procedure and KPIs	Review the data classification policy and procedure and KPIs	8 days	Data classification policy and procedure and KPIs

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
E-2	• Identify available (existing) data • Prepare a list of all business departments (mentioning at least the manager and first official) • Identify all data and their owners • Prepare a list of all data owned by these entities • Classification of data based on specific categories (sensitive personal data, legal, procurement, etc.)	Coordination of meetings with all departments	15 Days	Data inventory
E-3	Review all classified datasets and records to ensure they fit the rating assigned to them	Coordinate meetings with all Departments	12 days	Datasets and records that have been reviewed to ensure they are suitable for their rating
E-4	Advice on how to publish the classification levels assigned to the data sets،the population of this metadata shall be executed according to the process defined in the Metadata and Data Catalog Management domain under NDMO standards (if this is available)	Publish the rating scores given to datasets as they are in the Metadata and Data Catalog Management domain. (if this is available)	3 days	Rating scores given to datasets published (if this is available)

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
E-6	Advising on how to record a list of all selected datasets and records, as well as all activities carried out during the data classification procedure	Document all selected datasets and records in a combined record, capturing every activity undertaken throughout the data classification process.	Throughout the duration of the project	Aggregated record a list of all selected datasets and records, as well as all activities performed during the data classification process

Example of Data Inventory:



مجموعة البيانات (إلى أي م بيانات ينتمي هذا البيا Dataset	القسم/الإدارة التي يتبع لها ممثل بيانات الأعمال The department to which the business data representative reports	ممثل بيانات الاعمال (المالك) - داخل المنظمة Business Data Executive owner in the) (organization	الأدوار و المسؤوليات	علامات للبيان Tags	نوع البيان Data Type	توصيف بسيط عن البيان Brief Description	اسم الحقل (انجليزي) Name in English	اسم الحقل (عربي) Name in Arabic	معلومات أساسية عن البي	تسلسل خاص باسم الحقول Sequence ID
										قسم المراجعة الداخلية
بيانات تنظمية	Internal Audit	Cheif Internal auditor		charter	Strings	تحديد صلاحيات ال Audit مع كل الادارات و احقية الوصول للملفات	Audit Charter	ميثاق المراجعة		IA-0001
بيانات تنظمية	Internal Audit	Cheif Internal auditor		policy	Strings	مجموعة من القواعد التي تحدد كيفية تنفيذ التدقيق الداخلي والإجراءات	policies & procedures	السياسات والاجراءات		IA-0002
بيانات تنظمية	Internal Audit	Cheif Internal auditor		code_of_ethics	Strings	ثيقة تحدد المعايير الأخلاقية التي يجب على فريق التدقيق الداخلي	code of ethics of internal Auditor	ميثاق اخلاقيات المراجعة الداخلية		IA-0003
بيانات تنظمية البيانات القانونية	Internal Audit	Cheif Internal auditor		NDA	Strings , Numbers, Date	تعبير عن الالتزام بالحفاظ على سرية المعلومات التي يتعاملون معها	NDA	تعهد السرية		IA-0004
بيانات تنظمية	Internal Audit	Cheif Internal auditor		Risk	Strings and Numbers	عملية تحليل وتقييم المخاطر التي تؤثر على الشركة	Risk Assessment	تقييم المخاطر		IA-0005
بيانات تنظمية	Internal Audit	Cheif Internal auditor		plan	Strings , Numbers, Date	خطة المراجعة لكل الادارات على مدار ثلاث سنوات	audit plan	خطة المراجعة		IA-0006
بيانات تنظمية	Internal Audit	Cheif Internal auditor		announcement	Strings , Numbers, Date	إعلام الأقسام المختلفة بجدول التدقيق وأهدافه	Audit announcement	اشعار المراجعة		IA-0007
بيانات تنظمية	Internal Audit	Cheif Internal auditor		Requirements	Strings	المتطلبات التى تطلب من الادارات لعمل المراجعة	initial Requirements	المتطلبات الاولية		IA-0008
بيانات تنظمية	Internal Audit	Cheif Internal auditor		periodic	Strings , Numbers, Date	تقارير توثق النتائج المؤقتة لعملية التدقيق أثناء تنفيذها	periodic report	التقارير الدورية		IA-0009
بيانات تنظمية	Internal Audit	Cheif Internal auditor		KPI	Strings , Numbers, Date	معايير تستخدم لقياس أداء العمليات والمخاطر	KPI	مؤشرات الاداء		IA-0010

C490

السياسات والاجراءات

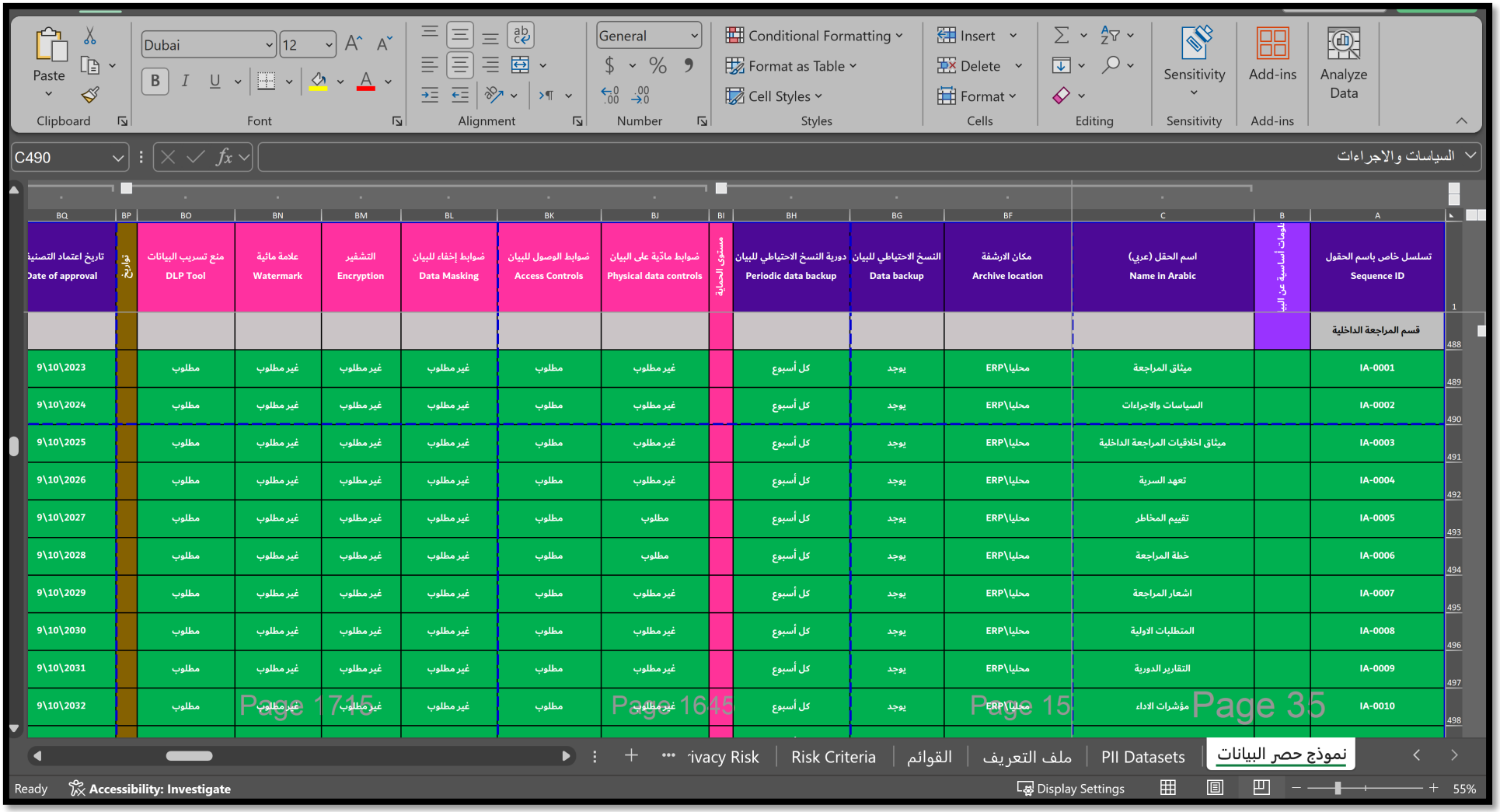
تسلسل خاص باسم الحقول Sequence ID	معلومات أساسية عن البيا	اسم الحقل (عربي) Name in Arabic	إمكانية مشاركة هذا البيان Possibility of sharing data	نوع صلاحية المشاركة Data sharing permission	طبيعة المشاركة Nature of data sharing	مكان حفظ البيان Storage Place	نوع مخزن البيانات الحاوي للبيان Data storage type	المصلحة الوطنية	هل سيخضع البيان لاهتمام وسائل الإعلام المحلية أو الدولية؟ وهل سيعطي انطباع سلبي؟	هل يشكل البيان خطرا على العلاقات مع الدول الصديقة؟ هل سيزيد من حدة التوتر الدولي؟ هل يمكن أن يؤدي إلى احتجاجات أو عقوبات من دول أخرى؟	في حال نشر البيان ، هل سيسا على تنظيم أعمال تخريبية أو ارتك جرائم خطيرة؟ هل يُشكل مصدر للجميع؟
قسم المراجعة الداخلية											
IA-0001		ميثاق المراجعة	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0002		السياسات والاجراءات	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0003		ميثاق اخلاقيات المراجعة الداخلية	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0004		تعهد السرية	لا يمكن	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0005		تقييم المخاطر	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0006		خطة المراجعة	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0007		اشعار المراجعة	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0008		المتطلبات الاولية	نعم - داخل الجهة فقط	اطلاع و اعتماد	باتجاهين	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0009		التقارير الدورية	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	لا
IA-0010		مؤشرات الاداء	نعم - داخل الجهة فقط	اطلاع	باتجاه واحد	يتم حفظها محليا على الجهاز Shared folder\	ملف pdf		لا	لا	65 لا

Page 595 Page 525 Page 45 Page 35

ivacy Risk | Risk Criteria | القوائم | ملف التعريف | PII Datasets | نموذج حصر البيانات

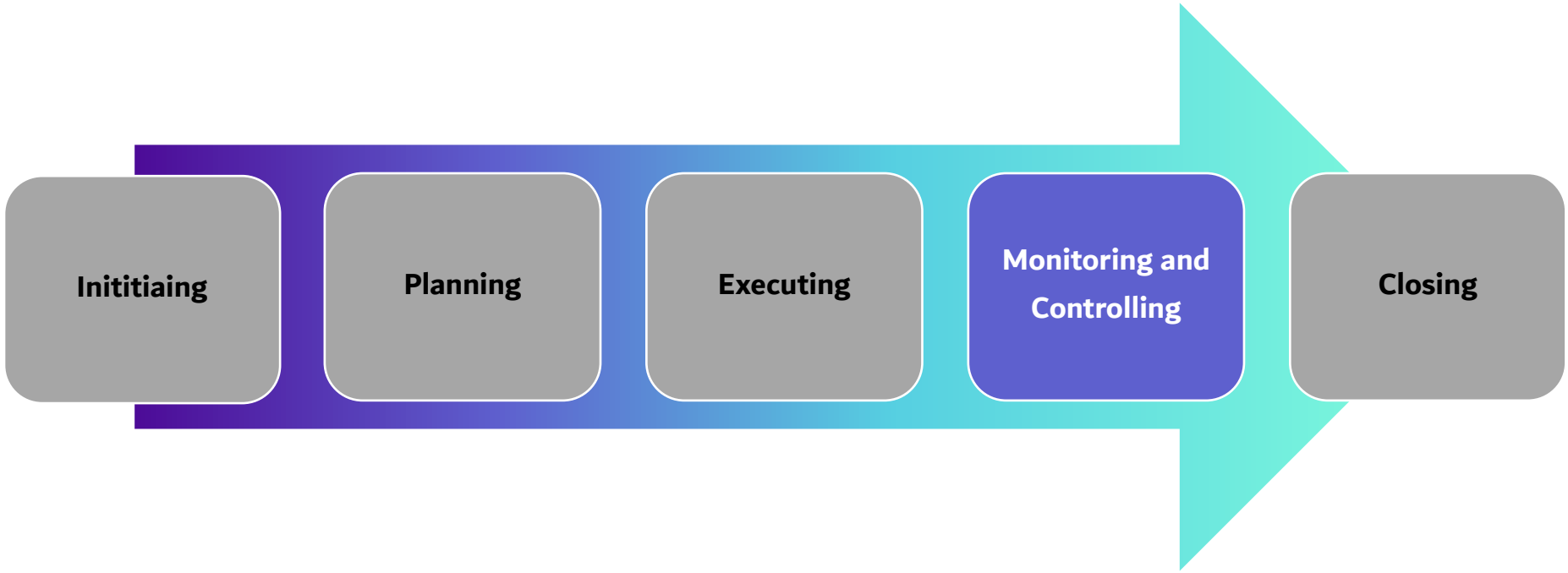
Ready Accessibility: Investigate Display Settings 55%


C490
السياسات والاجراءات
AL
AK
AJ
AI
AH
AG
C
B
A
نوع المعلومات الشخصية (عادية أم حساسة)
Type of Personal Identifiable Information (Normal or Sensitive)
هل سيؤدي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟
Will disclosing data reveal people's names, locations, etc.?
الأفراد
الأثر العام على مستوى أنشطة الجهة
The general impact on the level of the entity's activities
هل سيؤدي الكشف عن البيان إلى حدوث أضرار أو فقدان للدور الريادي التي تتمتع به الجهة أو خسارة أي من أصولها؟ أو تأثير بشكل سلبي على مهمات الجهة ؟ إنهاء عقود عددٍ كبيرٍ من الموظفين؟ يؤثر على القدرة التنافسية للجهة ؟
Imposing a negative impact on the entity's competitiveness?
هل سيؤدي الكشف عن البيان إلى خسائر مالية أو إفلاس الجهة ؟ أو خسارة أرباح ؟
Will disclosing data lead to financial losses or bankruptcy of the entity? Loss of profits?
اسم الحقل (عربي)
Name in Arabic
معلومات أساسية عن البيا
تسلسل خاص باسم الحقول
Sequence ID
1
قسم المراجعة الداخلية
488
-- | لا | لايوجد | لا | لا | ميثاق المراجعة | IA-0001 | 489
-- | لا | لايوجد | لا | لا | السياسات والاجراءات | IA-0002 | 490
-- | لا | لايوجد | لا | لا | ميثاق اخلاقيات المراجعة الداخلية | IA-0003 | 491
Sensitive - حساسة | لا | لايوجد | لا | لا | تعهد السرية | IA-0004 | 492
-- | لا | لايوجد | نعم بشكل قليل | لا | تقييم المخاطر | IA-0005 | 493
-- | لا | لايوجد | لا | لا | خطة المراجعة | IA-0006 | 494
-- | لا | لايوجد | لا | لا | اشعار المراجعة | IA-0007 | 495
-- | لا | لايوجد | لا | لا | المتطلبات الاولية | IA-0008 | 496
-- | لا | لايوجد | لا | لا | التقارير الدورية | IA-0009 | 497
1015 -- | لا | Page 945 | لايوجد | Page 875 | لا | Page 8 | مؤشرات الاداء | Page 35 | IA-0010 | 498
ivacy Risk | Risk Criteria | القوائم | ملف التعريف | PII Datasets | نموذج حصر البيانات
Ready
Accessibility: Investigate
Display Settings
55%



تاريخ اعتماد التصنيف Date of approval	فارغ	منع تسريب البيانات DLP Tool	علامة مائية Watermark	التشفير Encryption	ضوابط إخفاء للبيان Data Masking	ضوابط الوصول للبيان Access Controls	ضوابط مادّية على البيان Physical data controls	مستوى الحماية	دورية النسخ الاحتياطي للبيان Periodic data backup	النسخ الاحتياطي للبيان Data backup	مكان الارشفة Archive location	اسم الحقل (عربي) Name in Arabic	بيانات أساسية عن البيا	تسلسل خاص باسم الحقول Sequence ID
														قسم المراجعة الداخلية
9\10\2023		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	ميثاق المراجعة		IA-0001
9\10\2024		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	السياسات والاجراءات		IA-0002
9\10\2025		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	ميثاق اخلاقيات المراجعة الداخلية		IA-0003
9\10\2026		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	تعهد السرية		IA-0004
9\10\2027		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	مطلوب		كل أسبوع	يوجد	محليا\ERP	تقييم المخاطر		IA-0005
9\10\2028		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	مطلوب		كل أسبوع	يوجد	محليا\ERP	خطة المراجعة		IA-0006
9\10\2029		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	اشعار المراجعة		IA-0007
9\10\2030		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	المتطلبات الاولية		IA-0008
9\10\2031		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	التقارير الدورية		IA-0009
9\10\2032		مطلوب	غير مطلوب	غير مطلوب	غير مطلوب	مطلوب	غير مطلوب		كل أسبوع	يوجد	محليا\ERP	مؤشرات الاداء		IA-0010

1.4 Monitoring and Controlling Phase



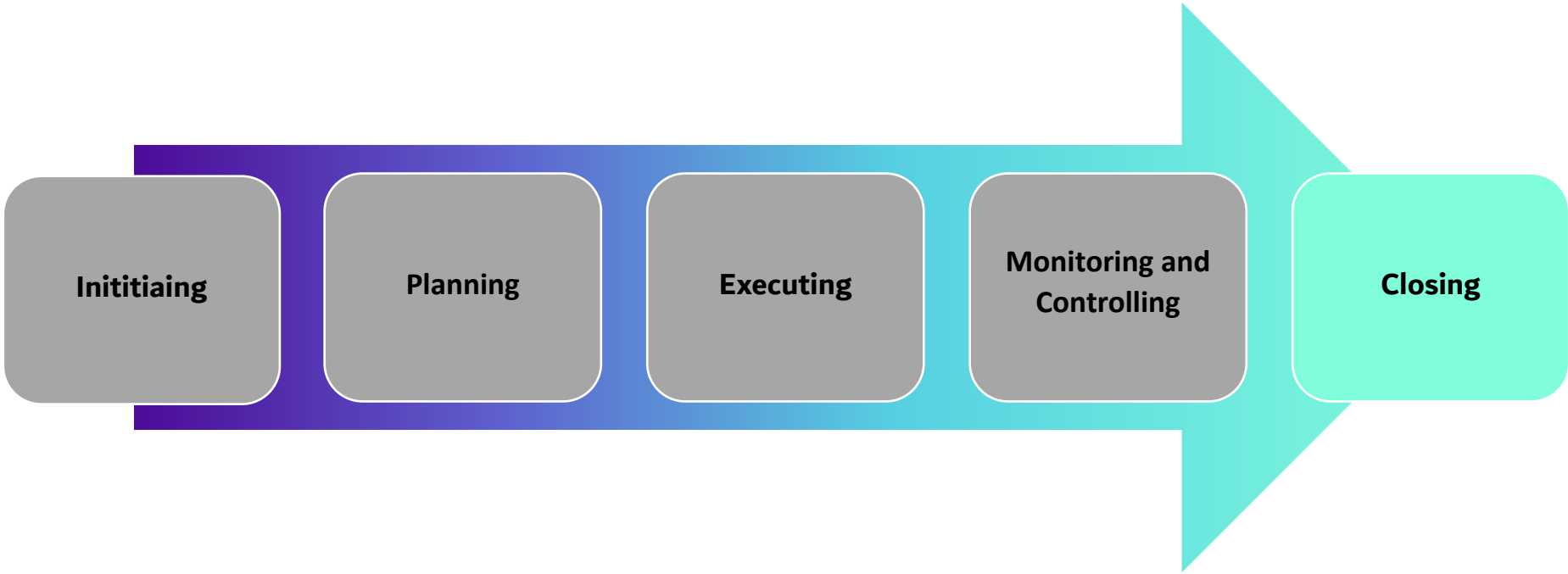
At this stage, the project work is monitored, performance and changes are monitored.

The table below also contains the activities that will be carried out at this stage:

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
M-1	Advising on how to establish protection and processing controls for each set of data and records according to their classification	The Cybersecurity Department will implement data protection controls with coordination of IT Department	7 Days	Filled Data Inventory with the proper security controls required for each dataset

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
M-2	Conducting an awareness workshop on data classification directed at all employees in the organization, aimed at introducing them to the basics of data classification.	Coordinate and facilitate the workshop.	1 day	Trained staff are aware of the importance and methodology of classifying data.

1.5 Closure phase



At this stage, we ensure the thorough verification of all project deliverables and the achievement of project objectives.

The table below also contains the activities that will be carried out at this stage:

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
C-1	Ensure that the deliveries are completed 1. Writing lessons learned. 2. Signing the project closure document.	1. Approval of deliverables 2. Co-writing lessons learned	5 days	1. Deliverables are completed and approved

#	Activities to be carried out by Trusted Vision	Activities to be carried out by the entity	Detailed timeline	Completed activities and materials delivered to the entity
		3. Signing the project closure document		2. Signed project closure document.

4. Project-related risks

The most important risks related to the project have been identified as in the table below

#	Risk scenario	Overall Level	Controls for dealing with risk
1	Lack of cooperation of the entity's employees and consequently a delay in deliveries	**High**	1. Assign a dedicated person from the entity, empowered to collaborate directly with the consultants. 2. Issue a directive from the authority holder mandating all departments to cooperate with consultants.
2	Disagreement with the documents delivered	**Medium**	Develop and activate a quality plan jointly between the company and the entity.
3	The unexpected resignation of a consultant during the project could disrupt project continuity.	**Low**	Providing other consultants for reserve by the company

5. Resource, Quality and Communication Plans

At the planning stage, the project manager develops a comprehensive suite of plans to ensure optimal project execution. These include:

- In the resource plan, the available resources are inventoried, requirements and priorities are determined, and resources are allocated according to priorities.
- In the quality plan, quality standards are defined for application in the project, such as workflow methods, time required to review documents (**three working days for 1 time**), and mechanisms for reviewing and approving documents.
- In the communication plan, identifies the most effective communication methods tailored to the needs of the stakeholders.

These plans are an important part of project management, and their goal is to determine how resources are prepared, quality management and how to communicate during the life of a project. It includes all stakeholder roles.

6. Project Management

During the project period, consultants will provide basic project management documents that include:

- Schedules and minutes of meetings
- Project Progress Reports

7. Project scope and assumptions

Outside the scope of work

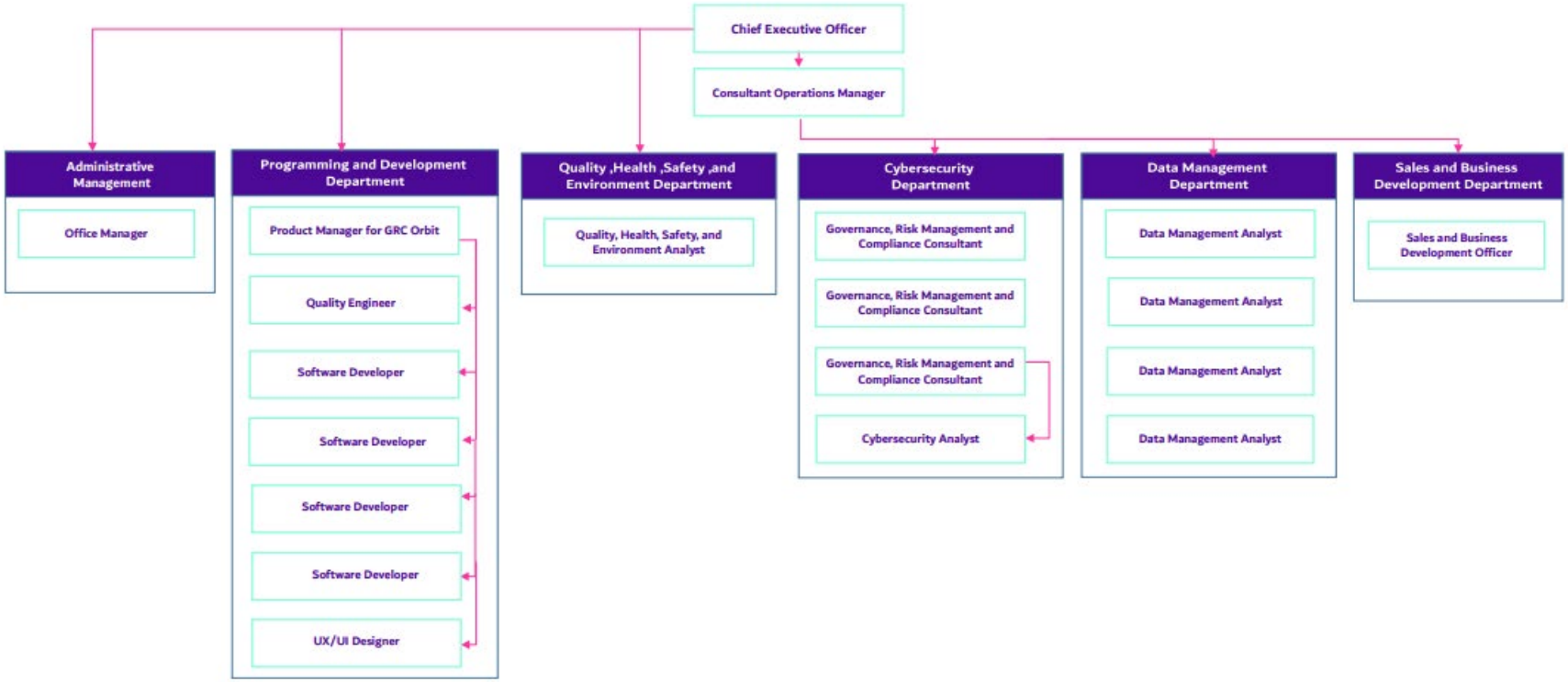
1. Implement or purchase technology tools and solutions related to the application of data management project.
2. Any other service not explicitly mentioned in the earlier sections will be considered outside the scope of work.

Assumptions

1. **All activities will take place during the project period only and the company has nothing to do with it if there is any delay or non-cooperation from the party**
2. **The company is not responsible for any delay that occurs on the part of the entity**
3. **The project will be executed for 3 months.**
4. **If there is no response within 30 days after the delivery of the policy and procedure, the project is considered completed.**
5. **Cooperation between departments of the entity is mandatory for the success of the project**

8. Company Information

Trusted Vision is a data management and cybersecurity consulting firm that provides full services in governance, risk, and compliance management, as well as solutions and training, to help entities meet their business requirements. What sets us apart are the core values we espouse.



9. Certificates

Our team holds a variety of certifications, including:


PECB
ISO 9001
LEAD AUDITOR
ITIL
FOUNDATION
CompTIA
CCAP
Cloud Admin
PROFESSIONAL
CompTIA
CSCP
Secure Cloud
PROFESSIONAL
CompTIA
Data+
CompTIA
Cloud+
CompTIA
CySA+
CompTIA
Network+
CompTIA
A+
CompTIA
Security+
CNSS
FORTINET
NSE
1
ASSOCIATE
FORTINET
NSE
2
ASSOCIATE
FORTINET
NSE
3
ASSOCIATE
FORTINET
NSE
4
PROFESSIONAL
C|EH
Certified Ethical Hacker
paloalto
NETWORKS
PCCSA
paloalto
NETWORKS
PCNSA
paloalto
NETWORKS
PCNSE
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA
CYBER+INFRASTRUCTURE
COMP
ASSOCIATE
CERTIFIED

11. Earlier Projects

Many projects have been implemented by dealing with various parties in different countries and multiple environments, and we always strive to implement the best practices and standards to achieve the best required results.

Project No.	Project Name	Client Name	Logo	Project Description
1	Implementation of the SAMA CSF Cybersecurity Framework	Gulf Union and Al Ahlia Insurance Company		1. Developing cybersecurity policies, procedures and standards issued by the Saudi Central Bank 2. Conducting a Cybersecurity Risk Assessment on information systems, assets, and processes 3. Developing key performance indicators and key risk indicators for operations (KPIs, KRIs) 4. Performing process monitoring
2	Implementing a Business Continuity Management System SAMA BCM	ASIG Insurance Company		1. Establish a Business Continuity Management System 2. Develop relevant policies, procedures, and standards. 3. Define and implement a Business Impact Analysis 4. Conduct a Business Continuity Risk Assessment

				5. Define a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) 6. Developing a Business Continuity Strategy 7. Develop Business Continuity Plans 8. Define Performance Metrics and KPIs
3	Implementation of Business Continuity and Disaster Recovery Program	Energy Manufacturing and Services Company (TAQA)		1. Establish a Business Continuity Management System 2. Develop relevant policies, procedures, and standards. 3. Define and implement a Business Impact Analysis 4. Conduct a Business Continuity Risk Assessment 5. Define a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) 6. Developing a Business Continuity Strategy 7. Develop Business Continuity Plans 8. Define Performance Metrics and KPIs
4	Implementation of ISO 27001 and basic cybersecurity controls (ECC, CCC, DCC, OSMACC, TCC)	Energy Manufacturing and Services Company (TAQA)		1. Establish a cybersecurity management system. 2. Develop a cybersecurity strategy and operational model. 3. Develop relevant policies, procedures, and standards.

				4. Ensure compliance with the National Cybersecurity Authority frameworks ECC, CCC, DCC, OSMACC, TCC 5. Ensure compliance with ISO 27001 6. Conduct internal audits on the National Cybersecurity Authority frameworks and ISO 27001 7. Obtain ISO 27001 certification
5	Audit and Oversee the Implementation of NCA-ECC Essential Cybersecurity Controls	Sovereign Government Entity		1. Improve governance documents (cybersecurity strategy, cybersecurity roles and responsibilities, cybersecurity policies) 2. Audit of core cybersecurity controls NCA-ECC
6	IT Systems Audit	Lebara Telecommunications Company	LEBARA ليبارا موبايل	IT Policies and Procedures Audit (General Technical Controls + Application Technical Controls)
7	ISO 27001 Information Security Standard Training	Energy Manufacturing and Services Company (Energy)	TAQA	Providing training in ISO 27001 information security standard

8	Data Management and Governance Strategy	King Abdulaziz Public Library		1. Conduct gap analysis on the national data governance and management framework. 2. Study the current situation. 3. Develop a data management strategy. 4. Develop an open data plan. 5. Publish six open data sets on the Saudi National Data Platform
9	Implementation of ISO 27001 Information Security Standard	Genelle	genelle	1. Establish an information security management system. 2. Develop relevant policies, procedures, and standards. 3. Ensure compliance with ISO 27001 4. Conduct remediation activities and resolve findings. 5. Obtain ISO 27001 certification
10	Saudi Aramco Cybersecurity Implementation	Maham	Maham مهام	1. Implement Aramco Cybersecurity Standard SACS-002 2. Develop relevant policies, procedures, and standards
11	Data Classification	Perfect Presentation	2P شركة العرض المتقن Perfect Presentation	1. Collect and classify all data. 2. Develop policies, procedures and standards related to data classification and protection

12	Implementation of ISO 27001 Information Security Standard and Basic Cybersecurity Controls (ECC, CCC, DCC, OSMACC, TCC)	National Community Development Program (Tanmia)	تنمية البرنامج الوطني للتنمية المجتمعية في المناطق	1. Establish a cybersecurity management system. 2. Develop a cybersecurity strategy and operational model. 3. Develop relevant policies, procedures, and standards. 4. Ensure compliance with the National Cybersecurity Authority frameworks ECC, CCC, DCC, OSMACC, TCC 5. Ensure compliance with ISO 27001 6. Conduct internal audits on the National Cybersecurity Authority frameworks and ISO 27001 7. Obtain ISO 27001 certification
13	Cybersecurity Risk Management	Sovereign Government Entity		1. Develop a cybersecurity risk management method and align it with the overall risk management method. 2. Conduct a cybersecurity risk assessment on information assets + third parties + material changes + technical projects + operations
14	NCA-ECC and CCC-P	Nashirnet		1. Establish a cybersecurity management system. 2. Develop policies, procedures, and standards for cloud computing controls

				and ECC + CCC core controls for service providers. 3. Conduct cybersecurity risk assessments for projects and products. 4. Conduct internal audits. 5. Develop and measure performance indicators
15	Data Classification and Modeling	King Abdulaziz Public Library		1. Develop data log. 2. Classify data. 3. Develop data modeling plan and perform modeling for library systems
16	Implementation of the Personal Data Protection Regulation (PDPL)	Aljaber Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy. 3. Developing consent management processes 4. Conducting audits of data processing activities 5. Conducting awareness workshops on personal data protection
17	Implementation of the Personal Data Protection Regulation (PDPL)	Hala Payment		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy.

				3. Developing consent management processes 4. Conducting audits of data processing activities 5. Conducting awareness workshops on personal data protection
18	Implementation of the Personal Data Protection Regulation (PDPL) Regulation	Mrna Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy. 3. Developing consent management processes 4. Conducting audits of data processing activities 6. Conducting awareness workshops on personal data protection
19	Implementation of SAMA CSF	Finzey		1. Conduct a comprehensive cybersecurity gap assessment. 2. Develop policies, procedures, and standards in alignment with the Saudi Central Bank (SAMA) Cybersecurity Framework. 3. Perform cybersecurity risk assessments for all information assets. 4. Establish and check cybersecurity performance indicators (KPIs.

				5. Development of a comprehensive Disaster Recovery (DR) Plan and Incident Response (IR) Plan
20	Implementation of the Personal Data Protection Law and Regulation (PDPL)	Finzey	فينزي للتمويل FinZev Finance	1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy 3. Developing consent management processes 4. Conducting audits of data processing activities 6. Conducting awareness workshops on personal data protection
21	Data Classification	Finzey	فينزي للتمويل FinZev Finance	1. Collect and classify all data 2. Develop policies, procedures and standards related to data classification and protection

12. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	H. A	Business Regulatory, Governance and Risk Management (GRC) Advisor to the CEO	Bachelor of Computer Engineering	13 Years	1. Manage and conduct operational and operational reviews in compliance with Saudi Arabian Oil Company (SAS 002), ISO 27001, NCA-ECC and NIST SP 800-53 cybersecurity requirements. 2. Manage and develop customized cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA and Saudi Arabian Oil Company Cybersecurity Standard. 3. Manage cybersecurity risks and conduct cybersecurity risk assessments and IT risk assessments by national and international standards.

					4. Implement and review the organization's Information Security Management System by ISO 27001 and the National Cybersecurity Authority (NCA-KSA) 5. Managing and implementing the organization's business continuity management system according to ISO 22301
2	B. A	Governance and Risk Management (GRC) Consultant	Master of Cyber security	2 Years	1. Manage and conduct operational and business reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards.

					3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the organization's Information Security Management System based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.
3	G.H	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	3 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53.

					2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the company's cybersecurity management system based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.

4	A. Y	Governance and Risk Management (GRC) Consultant	Master of Cybersecurity	2 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.
5	I.A	Governance and Risk Management (GRC) Consultant	Bachelor of Software Engineering	15 Years	1. Design, implement, and oversee data governance frameworks, ensuring adherence to regulations such as SDAIA guidelines, and GDPR. 2. Develop data management strategies, policies, and initiatives aligned with organizational aims and best international practices.

					3. Establish and enforce data quality standards to enhance accuracy, integrity, and reliability. 4. Evaluate existing data processes and recommend enhancements to improve workflow efficiency. 5. Create dashboards and generate reports to support data-driven decision-making. 6. Collaboration and Coordination: Partner with IT, operations, and business units to align data strategies with organizational goals.
8	B. B	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Information Systems	1 Year	1. Finding and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic aims. 2. Conducting assessments of data management maturity to find gaps and recommend improvements. 3. Developing Business Intelligence (BI) use cases and enhance user experience through data-driven insights.

					4. Designing and implementing plans, policies, and procedures for Master and Reference Data Management, Freedom of Information, Document and Content Management, and Data Value Realization in alignment with NDMO regulations.
9	B. A	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	25 Years	1. Overseeing the design of information and communications systems 2. Overseeing the implementation of ISO 27001 certification 3. Overseeing the implementation of communications and data transmission projects 4. Overseeing the implementation of three fiber optic projects to ensure data transmission system security.

					5. Overseeing the implementation of LAN and WAN networks and ensuring data transmission system security. 6. Overseeing the implementation of the SCADA network