TRUSTED VISION

Technical Proposal for Cybersecurity Audit and Compliance Assessment Services

Version 1.0

Date: 30-4-2026 AD

Prepared by: Trusted Vision for Cybersecurity Company

Contact Information

Please feel free to contact the following individuals for information about this document:

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

TRUSTED VISION

Table of Contents

1. Executive summary of client requirements

Trusted Vision is pleased to submit this technical proposal for the provision of Cybersecurity Audit and Compliance Assessment Services under the two-year call-off agreement.

Our proposed scope focuses on internal cybersecurity audits, compliance and gap assessments, and advisory support related to applicable regulatory, legal, and international cybersecurity standards.

The proposed services are designed to provide an independent view of the current compliance posture, identify gaps, assess the effectiveness of cybersecurity controls, and provide practical recommendations and corrective actions to support continuous improvement.

We believe that our experience in delivering similar cybersecurity audit, compliance assessment, and advisory engagements positions Trusted Vision as a qualified consulting partner for this project. Our value proposition is supported by:

1. Extensive experience in designing and implementing cybersecurity governance, audit, compliance, and risk management engagements.
2. A balanced combination of international and regional expertise in cybersecurity, data protection, and regulatory compliance.
3. A structured and effective project delivery methodology to address the project requirements in a timely, professional, and quality-driven manner.
4. Strong knowledge of international standards, regulatory frameworks, and industry best practices, including ISO/IEC 27001:2022, ISO/IEC 27701:2019, and relevant cybersecurity compliance frameworks.
5. Specialized cybersecurity and data protection consulting expertise to support practical, risk-based, and sustainable improvements.

Note: The cooperation of the entity, its management, and relevant employees is essential to ensure the successful delivery of this engagement.

We trust that our proposed consulting services meet the requirements of the tender, and we look forward to establishing a successful and mutually beneficial working relationship.

As this is a call-off agreement, Trusted Vision will apply the proposed methodology to each individual service request separately. Each request will be initiated, planned, executed, monitored, and formally closed based on its agreed scope, timeline, deliverables, and reporting requirements.

2. Scope of Work

The scope of this proposal covers the provision of Cybersecurity Audit and Compliance Assessment Services under the two-year call-off agreement. The services will be performed based on the specific request issued by the client for each call-off order, and will focus on assessing the implementation, effectiveness, and compliance status of cybersecurity controls within the client's IT cybersecurity environment.

The scope is aligned with the audit and compliance assessment requirements stated in the RFP, including Internal Audit and Compliance/GAP Assessments against applicable laws, regulations, standards, and cybersecurity frameworks such as ISO/IEC 27001:2022, ISO/IEC 27701:2019, Qatar Cyber Security Framework 2022, National Information Assurance Standard, Qatar Cyber Security Law, and Personal Data Privacy Law.

Cyber security audits and Compliance Assessments

Cyber security audits and compliance assessments will be based on international standards or country specific frameworks/guidelines. However, based on the organization conditions there will be more compliance requirements based on the strategical and technological changes.

14 of 2014 Qatar Cyber Security Law

13 of 2016 Personal Data Privacy Law

Qatar 2022 Cyber Security Framework

National Information Assurance Standard

ISO27001:2022 Standard

ISO27701:2019 Standard

The following are key cyber security audits and compliance assessments.

. Internal Audit - SO27001:2022, Qatar Cyber Security Framework, National Information Assurance Standard, Personal data Protection and Privacy Law, Qatar Information Classification Policy and any other compliance

assessment and audit requirements based on the technology, regulatory, laws and internation standards.

Compliance/GAP assessments - ISO27001:2022, Qatar Cyber Security Framework, National Information

Assurance Standard, Personal data Protection and Privacy Law, Qatar Information Classification Policy and any other

compliance assessment and audit requirements based on the technology, regulatory, laws and internation standards.

Cyber security Compliance Service

Provide adequate **consultancy and awareness** support for emerging technologies, compliance requirements perspective and sector specific requirements. Below are key services.

Customized security awareness - based on the present situation within the world and Qatar and judiciary systems, customized security awareness trainings for SJC Staff and IT staff (English and Arabic both Languages).

Cyber security consultancy support - Provide security consultancy support for emerging technologies, major changes in SJC IT environment, legal, regulatory and internation standards requirements

Emerging Technologies Security

- AI/ML Governance & Risk (bias, adversarial attacks, misuse, data privacy).
- Cloud Security & Data Sovereignty (ISO 27017/27018, Qatar NIA).
- API& Microservices Security (OWASP API Top 10, Zero Trust).
- IoT & Smart Building Security (segmentation, telemetry monitoring).
- Blockchain, Digital Identity, and Biometric Security Controls.
- New and Emerging Technology adoption report

Major IT Environment Changes

- Secure Change & Release Management (ISO 27001 A. 12, A. 14).
- Data Migration & Cloud Transformation Risk Assessments.
- Third-Party/Vendor Risk Management (ISO 27036, SLA clauses).
- Secure SDLC, DevSecOps, and Code Assurance (SAST/DAST integration).
- Business Continuity, Backup, and Disaster Recovery Readiness (ISO 22301).
- Change evaluation consultancy report

Legal & Regulatory Compliance (Qatar & International)

- Qatar PDPPL (Law 13/2016): lawful processing, breach reporting, consent.

- Right to Access Information Law (Law 9/2022): transparency vs. confidentiality.
- Qatar Cybersecurity Framework & NIA Standard: baseline ICT controls.
- GDPR: cross-border transfers, accountability, privacy by design.
- HIPAA (if health data involved): judicial medical records protection.
- NIS2 Directive: resilience, incident reporting, supply chain governance.

International Standards Alignment

- ISO/IEC 27001:2022: ISMS implementation & risk-based approach.
- ISO/IEC 42001: Al Governance & Responsible Use.
- ISO/IEC 27701: Privacy Information Management.
- NIST Cybersecurity Framework: risk-based security maturity.
- NIST AI RMF: govern/map/measure/manage emerging Al risks.

1. In-Scope Services

No.	Service Area	Description
1	Internal Cybersecurity Audit	Conduct internal audits to assess the design, implementation, and effectiveness of cybersecurity controls against the agreed audit criteria.
2	Compliance/GAP Assessment	Assess the current compliance posture against applicable regulatory, legal, and international cybersecurity standards and identify gaps.

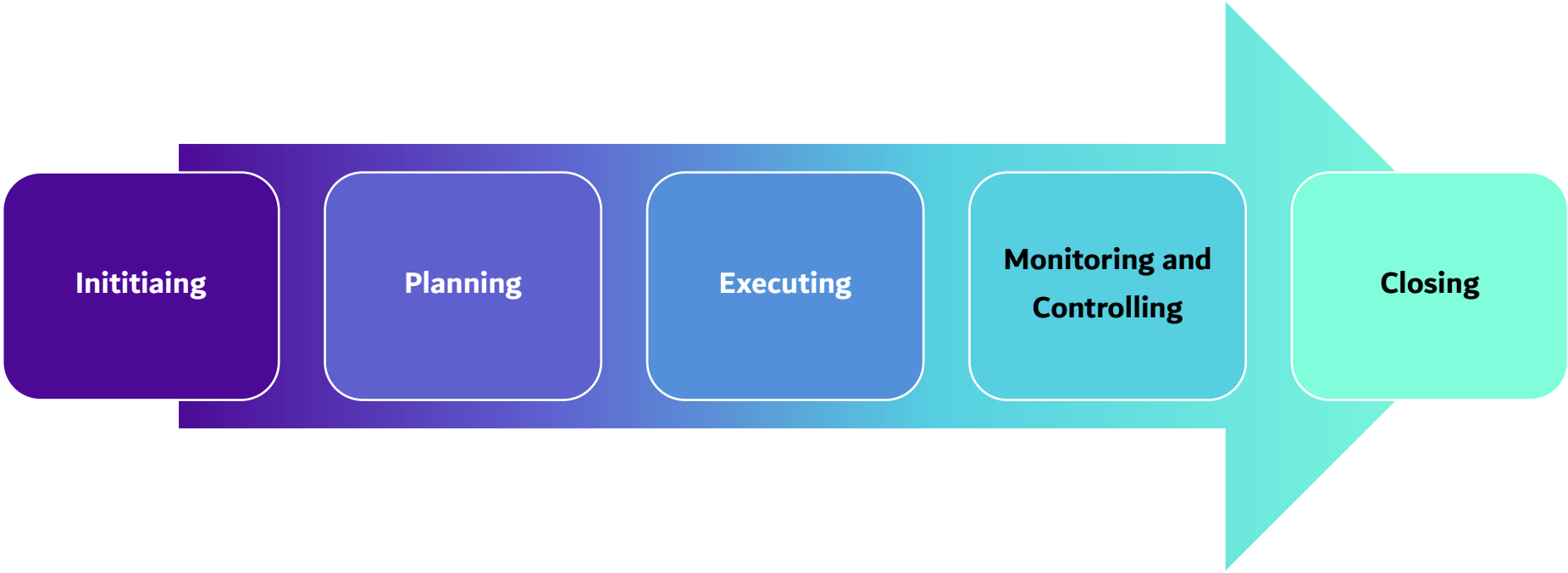
3	Audit Planning	Develop an audit plan for each call-off request, including scope, objectives, audit criteria, timeline, stakeholders, and evidence requirements.
4	Document and Evidence Review	Review relevant policies, procedures, standards, records, registers, reports, and supporting evidence provided by the client.
5	Stakeholder Interviews and Walkthroughs	Conduct interviews and walkthrough sessions with relevant control owners and stakeholders to validate control implementation.
6	Control Assessment	Evaluate cybersecurity controls to determine whether they are adequately designed, implemented, maintained, and aligned with applicable requirements.
7	Findings Identification	Identify positive findings, nonconformities, gaps, observations, risks, and improvement opportunities.
8	Recommendations and Corrective Actions	Provide practical recommendations and proposed corrective actions to address identified gaps and improve compliance maturity.
9	Reporting	Prepare audit and assessment reports, including detailed findings, risk implications, executive summary, and recommended action plan.
10	Closure and Presentation	Present the audit results to the client, discuss key findings, agree on next steps, and close the engagement formally.
11	Customized security awareness	based on the present situation within the world and Qatar and judiciary systems, customized security awareness trainings for SJC Staff and IT staff (English and Arabic both Languages).
12	Cyber security consultancy support	Provide security consultancy support for emerging technologies, major changes in SJC IT environment, legal, regulatory and internation standards requirements

2. Key Deliverables

The expected deliverables may include the following, depending on the specific call-off request:

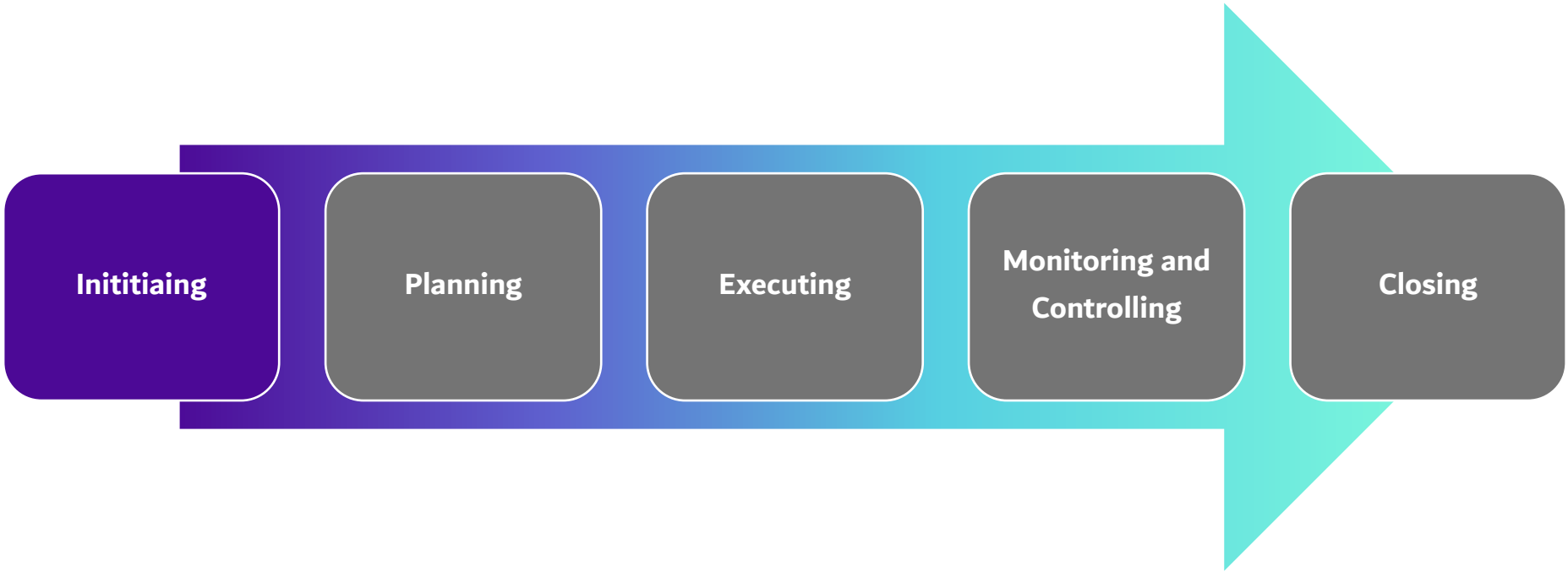
1. Audit Plan
2. Compliance/GAP Assessment Plan
3. Evidence Request List
4. Compliance Assessment Checklist
5. Document Review Log
6. Findings Register
7. Detailed Audit Report
8. Detailed Compliance/GAP Assessment Report
9. Executive Summary
10. Corrective Action Plan
11. Closing Meeting Minutes
12. Engagement Closure Note
13. Awareness session
14. Consultancy sessions , reports

3. Project Implementation Methodology



We at Trusted Vision follow the global project management methodology of the Project Management Institute (PMI) in terms of initiating, planning, executing, monitoring, and controlling, and closing.

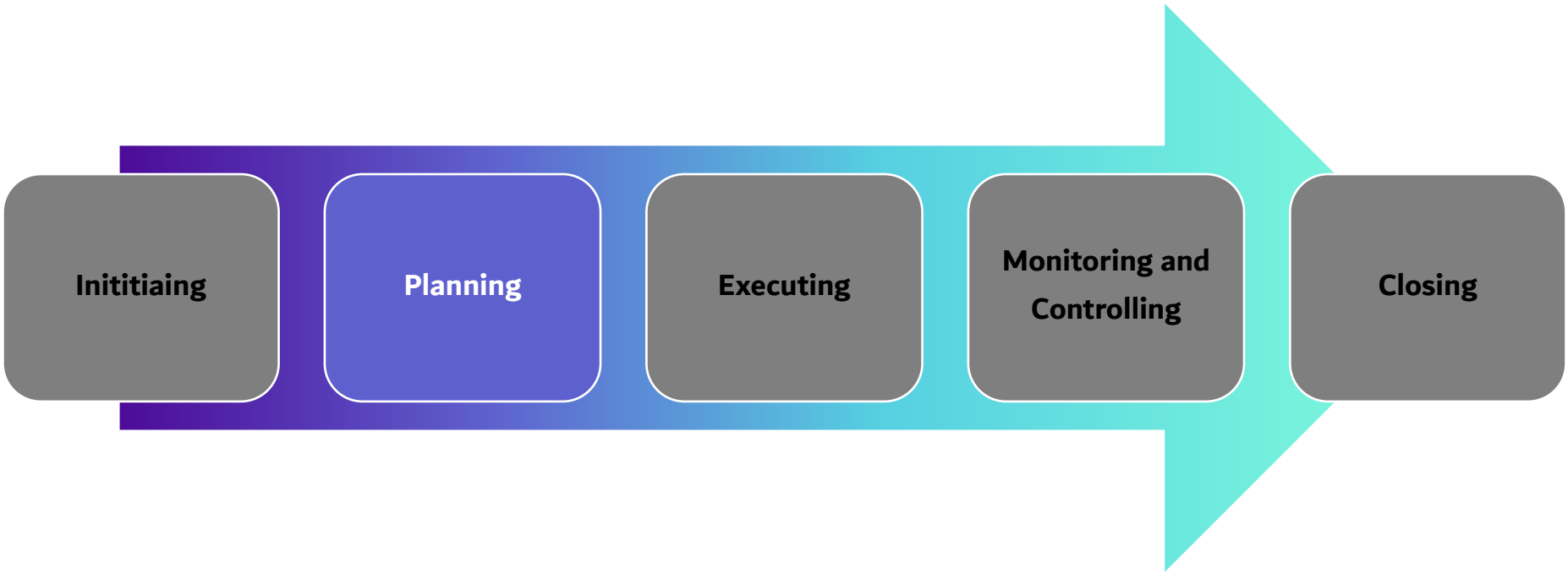
6.1 Initiating Phase



During this phase, the engagement is formally initiated by confirming the scope, objectives, stakeholders, project team, communication channels, and overall governance structure.

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Assign the project manager and audit team.	Nominate project sponsor, focal point, and relevant stakeholders.	Project team list and stakeholder list.
2	Confirm audit objectives, scope, applicable standards, and call-off requirements.	Confirm the required audit scope and applicable compliance frameworks.	Confirmed audit scope and engagement objectives.
3	Conduct a kick-off meeting to explain the audit approach, timeline, evidence requirements, and communication channels.	Arrange attendance of relevant stakeholders.	Kick-off meeting minutes and action items.

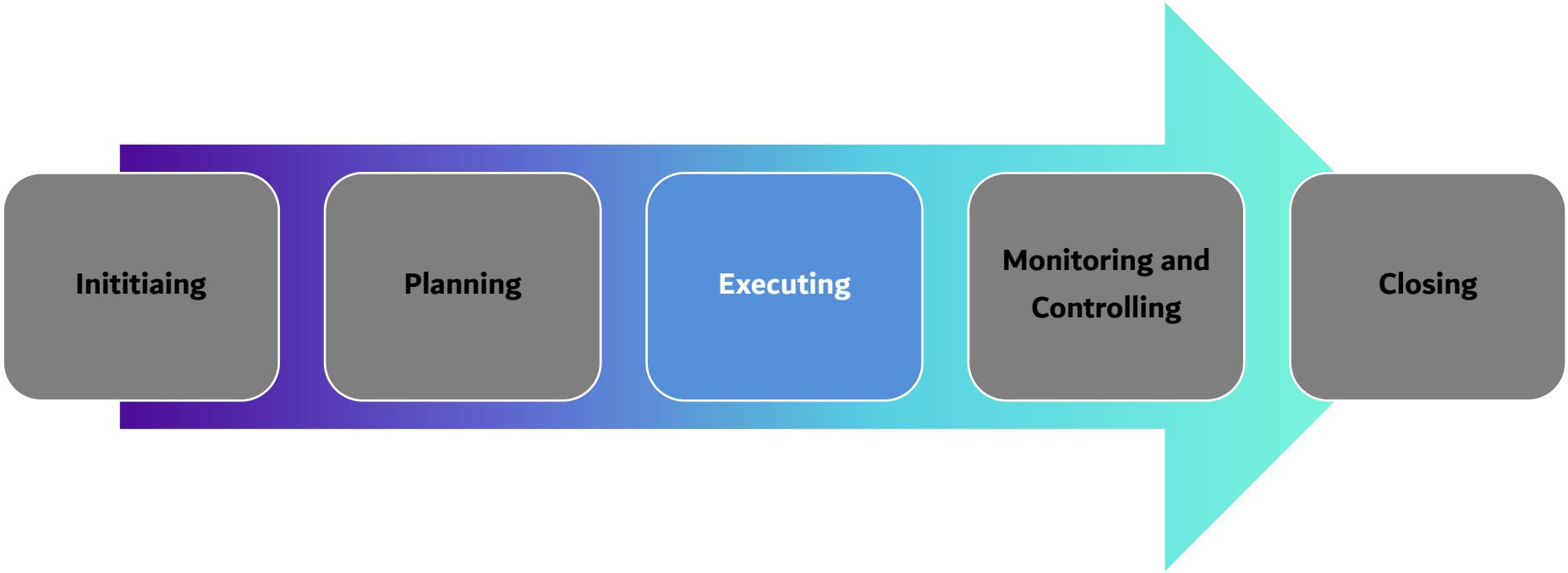
6.2 Planning Phase



During this phase, the audit and compliance assessment activities are planned in detail, including the audit criteria, timelines, evidence requirements, stakeholder interviews, and expected deliv0erables.

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Develop the audit plan, including audit scope, criteria, timeline, stakeholders, and evidence requirements.	Review and approve the audit plan.	Audit Plan.
2	Prepare the compliance assessment checklist based on the applicable standards and regulatory requirements.	Confirm applicable frameworks and provide relevant internal requirements.	Compliance Assessment Checklist.
3	Request and review initial documentation, including policies, procedures, registers, previous reports, and evidence.	Provide required documents and evidence.	Evidence Request List and Document Review Log.
4	Schedule interviews and workshops with relevant stakeholders.	Coordinate interviews and ensure availability of stakeholders.	Interview Schedule.

6.3 Executing Phase

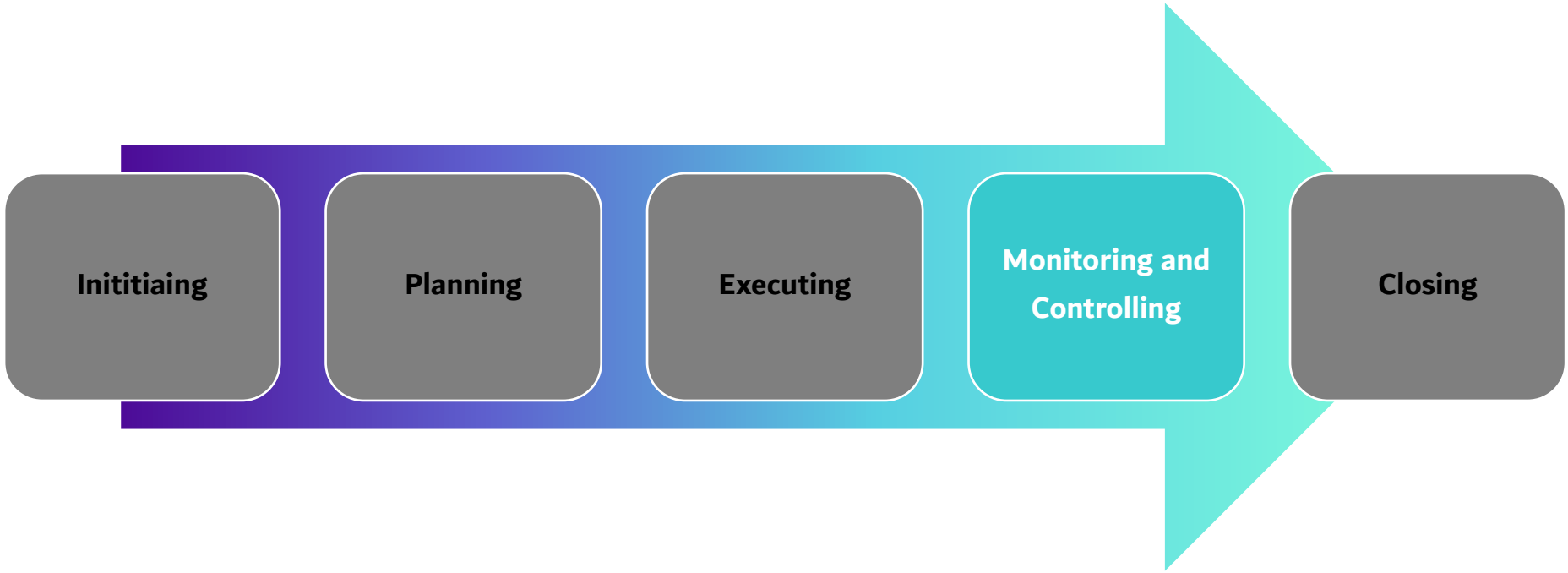


During this phase, the agreed audit and compliance assessment activities are performed through document review, evidence validation, stakeholder interviews, and control effectiveness assessment.

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Conduct document review against the agreed audit criteria.	Provide policies, procedures, records, and supporting evidence.	Document Review Results.
2	Conduct interviews and walkthroughs with control owners and relevant stakeholders.	Participate in interviews and provide clarifications.	Interview Notes and Evidence Log.
3	Evaluate the design and operating effectiveness of cybersecurity controls.	Provide additional evidence where required.	Control Assessment Results.
4	Identify compliance gaps, nonconformities, observations, and improvement opportunities.	Validate factual accuracy of findings.	Draft Findings Register.
5	Assess gaps against applicable frameworks such as ISO/IEC 27001:2022, ISO/IEC 27701:2019, Qatar Cyber Security Framework, National Information Assurance Standard, and relevant laws.	Confirm applicability and provide supporting documentation.	Compliance/GAP Assessment Results.
	Execute Customized security awareness - based on the present situation within the world and Qatar and judiciary systems, customized security awareness trainings for SJC Staff and IT staff (English and Arabic both Languages).	Determine the subjects to deliver the sessions Determine the number of sessions Determine the language to deliver the sessions	Sessions, presentations materials

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
	Provide security consultancy support for emerging technologies, major changes in SJC IT environment, legal, regulatory and internation standards requirements	Determine the subjects , the kind of delivery (sessions , reports , evaluations, etc)	Sessions, reports , etc

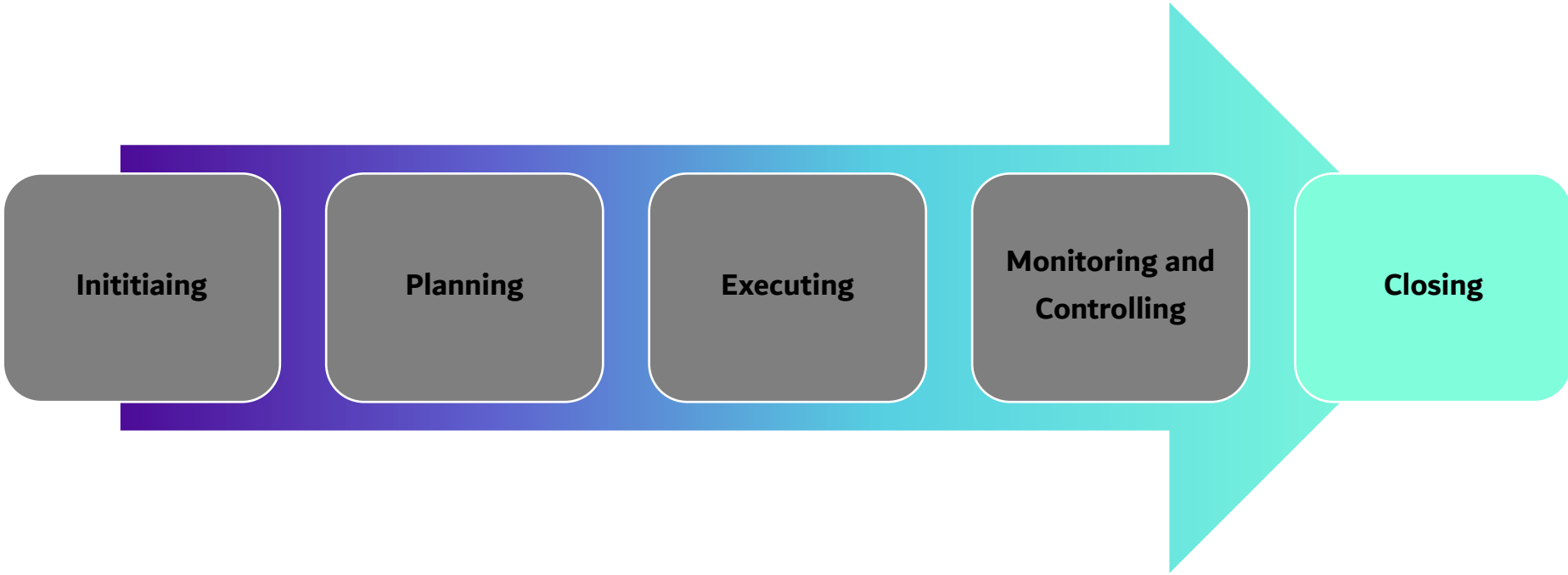
6.4 Monitoring and Controlling Phase



During this phase, the progress of the engagement is monitored against the approved plan, while issues, pending evidence, risks, findings, and required clarifications are tracked and managed.

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Monitor progress against the approved audit plan and timeline.	Attend progress meetings and provide required feedback.	Progress Updates.
2	Provide status updates on completed activities, pending evidence, issues, and risks.	Support in resolving pending evidence or access issues.	Weekly / Periodic Status Report.
3	Track findings, evidence status, and open clarifications.	Respond to clarification requests and validate findings.	Findings Tracker and Evidence Tracker.
4	Manage changes to scope or timeline, where required, through the agreed change process.	Review and approve any required changes.	Change Requests, if applicable.
5	Prepare and submit the draft audit or assessment report.	Review the draft report and provide comments.	Draft Audit / Assessment Report.
6	Update the report based on client feedback and finalize the findings and recommendations.	Validate factual accuracy and approve final comments.	Final Detailed Audit / Assessment Report.
7	Prepare an executive summary highlighting key findings, risks, and recommended actions.	Review and approve the executive summary.	Executive Summary.

6.5 Closing phase



During this phase, the final findings, reports, recommendations, and executive summary are completed, presented, approved, and formally closed with the client.:

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Conduct a closing meeting to present results, findings, and corrective action priorities.	Attend the closing meeting and agree on next steps.	Closing Meeting Minutes.
2	Submit final deliverables and close the call-off engagement.	Approve deliverables and confirm closure.	Engagement Closure Note.

4. Project scope and Assumptions

4.1 Outside the Scope of Work

Unless explicitly requested and agreed through a separate call-off request, the following activities are considered outside the scope of this proposal:

1. Implementation, purchase, or licensing of technical tools, systems, or cybersecurity solutions.
2. Remediation implementation or direct configuration changes on the entity's systems, applications, or infrastructure.
3. Any activity, service, or deliverable not explicitly mentioned in the agreed scope of work or call-off request.

4.2 Assumptions

1. **All The proposed services are based on the following assumptions:**
2. **The services will be delivered under a call-off agreement, and each request will have a clearly defined scope, timeline, deliverables, and required level of effort.**
3. **All activities will be performed within the agreed period for each call-off request.**
4. **The entity will provide the required documents, evidence, access, information, and stakeholder availability in a timely manner.**
5. **Cooperation from the entity's relevant departments and employees is essential for the successful completion of the engagement.**
6. **Trusted Vision shall not be responsible for delays caused by late responses, lack of cooperation, unavailability of required evidence, or delays from the entity's side.**

TRUSTED VISION

7. Any changes to the approved scope, timeline, or deliverables shall be managed through a formal change request and mutual agreement.
8. The review of deliverables and provision of comments by the entity shall be completed within the agreed review period.
9. The final timeline for each engagement will depend on the nature of the requested service, availability of information, and complexity of the audit or assessment.

5. Certificates

Our team holds a variety of certifications, including:

PECB ISO/IEC 27001 SENIOR LEAD IMPLEMENTER

PECB ISO/IEC 27001 SENIOR LEAD AUDITOR

PECB ISO/IEC 27032 LEAD CYBERSECURITY MANAGER

PECB ISO/IEC 38500 LEAD IT CORPORATE GOVERNANCE MANAGER

PECB ISO 31000 LEAD RISK MANAGER

PECB ISO/IEC 27005 SENIOR LEAD RISK MANAGER

PECB DATA PROTECTION OFFICER

PECB ISO 22301 FOUNDATION

PECB ISO/IEC 20000 FOUNDATION

PECB ISO 45001 LEAD AUDITOR

PECB ISO 14001 LEAD AUDITOR

PECB ISO 9001 LEAD IMPLEMENTER

TRUSTED VISION

6. Previous 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	إتحاد الخليج للتأمين التعاوني GULF UNION COOPERATIVE INSURANCE CO.	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	ACIG للتأمين بأمان	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. Develop 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. Develop 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 methodology and align it with the overall risk management methodology 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 Law and Regulations (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 Law and Regulations (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 Law and Regulation (PDPL)	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

				5. Conducting awareness workshops on personal data protection
19	Implementation of SAMA CSF	Finzey	فينزي للتمويل FinZev Finance	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		1. Collect and classify all data

			فينزي للتمويل FinZey Finance	2. Develop policies, procedures and standards related to data classification and protection
22	Supervise the implementation of General Data Protection Regulation (GDPR) requirements.	Genelle	genelle	1. Review of policies, procedures, and supporting documentation related to GDPR requirements. 2. Review and validation of Data Protection Impact Assessments (DPIAs). 3. Monitor compliance with data protection and privacy requirements in accordance with GDPR 4. Coordinate with relevant stakeholders and escalate observations to management.
23	Implement ISO 42001 for the Artificial Intelligence Management System (AIMS).	Genelle	genelle	1. Establish an Artificial Intelligence Management System (AIMS). 2. Develop related policies, procedures, and standards. 3. Ensure compliance with ISO 42001 requirements. 4. Perform audit activities against ISO 42001 requirements to assess compliance and identify gaps.

				5. Implement corrective actions and address findings/observations.
24	Microsoft Tools Assessment Project – DLP and Data Classification, Saudi Tourism Authority	Saudi Tourism Authority	SAUDI TOURISM AUTHORITY الهيئة السعودية للسياحة	1. Assess the capabilities of Microsoft tools in data classification and protection of sensitive information. 2. Review Data Loss Prevention (DLP) settings and policies within the Microsoft 365 environment. 3. Analyze data classification mechanisms and the implementation of Sensitivity Labels across files and emails. 4. Evaluate the effectiveness of data loss prevention controls across email, SharePoint, OneDrive, and Teams. 5. Review data protection policies and controls to ensure alignment with privacy and information security requirements. 6. Identify gaps and observations related to data classification and data loss prevention. 7. Provide recommendations to enhance DLP policies and strengthen the protection of sensitive data.

25	Cybersecurity and Data Privacy Audit Project – NCA ECC & PDPL	Tharwa		1. Conduct cybersecurity audits against National Cybersecurity Authority (NCA) ECC controls and applicable cybersecurity frameworks. 2. Perform data protection and privacy audits to assess compliance with Personal Data Protection Law requirements.
26	Enterprise Cybersecurity Audit – NCA Framework	Infratech		1. Conduct comprehensive cybersecurity audits against National Cybersecurity Authority frameworks, including ECC, DCC, CSCC, OSMACC, and CCC controls. 2. Assess the effectiveness of implemented cybersecurity controls, identify gaps and non-compliance areas, and evaluate alignment with NCA regulatory requirements. 3. Provide detailed audit reports and actionable recommendations, including remediation plans to enhance cybersecurity posture and ensure full compliance with NCA standards.

7. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	S.	Governance and Risk Management (GRC)	Bachelor of Computer Engineering	6 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	5 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
10	E.A	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.