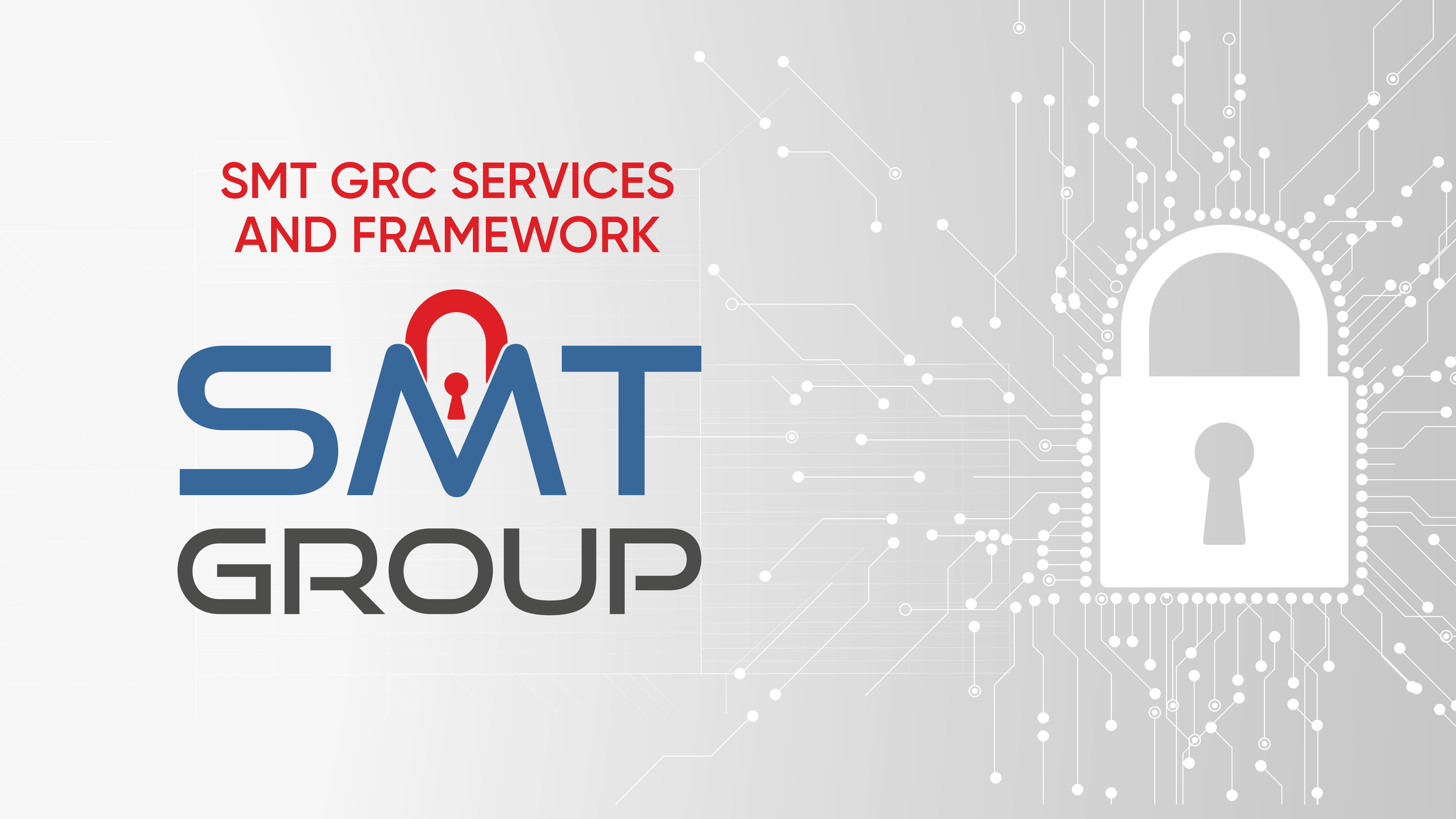
SMT GRC SERVICES AND FRAMEWORK

SMT GROUP



OUR COMPANY

SMT IS AN END-TO-END INFORMATION SECURITY SOLUTIONS PROVIDER & WELL ESTABLISHED COMPANY BASED IN

SMT STRONG TEAM OF HIGHLY QUALIFIED CONSULTANTS, CERTIFIED AND WELL-TRAINED TECHNICAL ENGINEERS WHO ARE CAPABLE OF UNDERSTANDING OUR CUSTOMERS' NEEDS IN ORDER TO MAKE SURE PROVIDING THEM WITH THE RIGHT TECHNOLOGY AND WORLD-CLASS SERVICES SURROUNDING TODAY'S IT/IS MATTERS THAT ALLOW LARGE, MID-SIZED AND SMALL COMPANIES TO MAINTAIN AND SAFEGUARD THEIR BUSINESS-CRITICAL OPERATIONS

OUR COMPANY

SOLUTION

1. SECURITY INFORMATION AND EVENT MANAGEMENT
2. ADVANCED MALWARE PROTECTION
3. CHANGE AUDITING
4. APPLICATION SECURITY
5. PRIVILEGED ACCESS MANAGEMENT
6. IDENTITY ACCESS MANAGEMENT
7. VULNERABILITY SCANNING

SERVICES AND CONSULTATION – ISO SERVICES – PCI SERVICES – SECURITY OPERATION CENTER – IT/SECURITY OUTSOURCE SERVICE • TRAINING – EC-COUNCIL – PECB – LINUX FOUNDATION – COMPTIA – AXELOS – PEOPLECERT –ISACA

SMT COMPETITIVE ADVANTAGES

CERTIFIED SERVICES

SMT IS FULLY CERTIFIED IN ALL SERVICES PROVIDED TO CUSTOMERS, ENSURING COMPLIANCE WITH INTERNATIONAL AND LOCAL STANDARDS.

SPECIALIZED SECURITY DEPARTMENTS

SMT HAS MULTIPLE DEDICATED DEPARTMENTS SPECIALIZED IN DIFFERENT AREAS OF CYBERSECURITY FOR STRONGER COMPLIANCE

EXPERT SUPPORT

INDEPENDENT SPECIALIZED DEPARTMENTS PROVIDES CONSULTATION AS A SERVICE BASED ON INTERNATIONAL STANDARDS, THERE BY DELIVERING

WHAT IS GRC (GOVERNANCE, RISK, AND COMPLIANCE)?

GOVERNANCE

GOVERNANCE REFERS TO THE FRAMEWORK & STANDARDS AND PROCESSES ORGANIZATIONS USE TO ENSURE THEY MEET STRATEGIC OBJECTIVES AND COMPLY WITH REGULATIONS WHILE MAINTAINING ACCOUNTABILITY

GOVERNANCE INVOLVES:

-ESTABLISHING POLICIES

-DEFINING ROLES AND RESPONSIBILITIES

-ALIGNING BUSINESS PRACTICES WITH ETHICAL STANDARDS AND ORGANIZATIONAL GOALS

-INTEGRATING SECURITY ACROSS ALL DEPARTMENTS

RISK

RISK REFERS TO THE POTENTIAL FOR EVENTS OR CONDITIONS THAT COULD NEGATIVELY IMPACT AN ORGANIZATION'S OBJECTIVES, ASSETS, REPUTATION, OR OPERATIONS

RISK MANAGEMENT INVOLVES:

-IDENTIFYING, ANALYZING AND ASSESSING RISKS

-MITIGATING RISKS MONITORING AND REPORTING

-AMEASURING THE EFFECTIVENESS OF THE EXISTING CONTROLS

-RISK TREATMENT PLAN

COMPLIANCE

COMPLIANCE REFERS TO THE ADHERENCE TO LAWS, REGULATIONS, INDUSTRY STANDARDS, AND INTERNAL POLICIES RELEVANT TO AN ORGANIZATION'S OPERATIONS

COMPLIANCE INVOLVES:

-LEGAL AND ETHICAL

-STAKEHOLDER TRUST

-NATIONAL REGULATIONS

GOVERNANCE SERVICES

WE PROVIDE GOVERNANCE SERVICES TO HELP ORGANIZATIONS ESTABLISH A STRUCTURED AND EFFECTIVE

GOVERNANCE SERVICES INCLUDE :

1. DEVELOP AND IMPLEMENT SECURITY POLICIES AND PROCEDURES TO PROVIDE A CLEAR REFERENCE
2. DELIVER SECURITY AWARENESS AND TRAINING PROGRAMS TO REDUCE HUMAN ERRORS
3. DEFINE ROLES AND RESPONSIBILITIES TO AVOID OVERLAPS OR GAPS
4. PROVIDE MANAGEMENT DASHBOARDS AND REPORTS FOR VISIBILITY AND DECISION-MAKING

RISK MANAGEMENT SERVICES

WE SUPPORT ORGANIZATIONS IN PROACTIVELY MANAGING CYBERSECURITY AND COMPLIANCE RISKS TO SAFEGUARD CRITICAL ASSETS AND ENSURE INFORMED DECISION MAKING

RISK MANAGEMENT SERVICES INCLUDE :

1. RISK IDENTIFICATION AND ASSESSMENT
2. ASSET-BASED AND SCENARIO-BASED RISK ASSESSMENTS
3. RISK TREATMENT PLANNING AND MITIGATION STRATEGIES
4. RISK MONITORING AND REPORTING

COMPLIANCE SERVICES

WE ENABLE ORGANIZATIONS TO ACHIEVE AND MAINTAIN COMPLIANCE WITH REGULATORY AND INDUSTRY

COMPLIANCE SERVICES INCLUDE :

1. CONDUCT GAP ASSESSMENTS AGAINST STANDARDS AND REGULATIONS(ISO/IEC 27001, ISO 22301, PCI DSS, SAMA, ETC.)
2. PERFORM INTERNAL AUDITS AND READINESS ASSESSMENTS
3. DEVELOP REMEDIATION AND CORRECTIVE ACTION PLANS
4. SUPPORT REGULATORY AND SUPERVISORY REPORTING REQUIREMENTS
5. PREPARE ORGANIZATIONS FOR CERTIFICATIONS SUCH AS ISO AND OTHERS

COMPLIANCE SERVICES VS. GRC SERVICES

COMPLIANCE

THESE SERVICES FOCUS ON HELPING AN ORGANIZATION **FOLLOW LAWS AND INDUSTRY STANDARDS.** THE MAIN GOAL IS TO **IMPLEMENT REGULATIONS AND DEMONSTRATE FORMAL COMPLIANCE.** EXAMPLES INCLUDE GDPR PROGRAMS, ISO CERTIFICATIONS, AND REGULATORY REPORTING

COMPLIANCE = FOCUSED ON LAWS AND STANDARDS

VS

GRC

THESE SERVICES ARE BROADER BECAUSE THEY **COVER ALL ASPECTS OF MANAGING THE ORGANIZATION SAFELY AND EFFECTIVELY**. NOT ONLY COMPLIANCE, BUT ALSO **GOVERNANCE** (HOW THE ORGANIZATION IS MANAGED) AND **RISK MANAGEMENT** (IDENTIFYING AND HANDLING RISKS) ARE INCLUDED. THE GOAL IS TO ORGANIZE THE COMPANY, MANAGE RISKS, AND EMBED COMPLIANCE INTO DAILY OPERATIONS.

GRC = THE FULL SYSTEM: HOW WE RUN THE COMPANY, MANAGE RISKS, AND FOLLOW THE RULES ALL TOGETHER

GRC – INTERNAL VS SERVICE PROVIDER

GRC WITHIN SMT (INTERNAL DEPARTMENT)

CORE SERVICES:

ISO IMPLEMENTATION & UPGRADES: FOR EXAMPLE ISO 27001 & ISO 22301 IMPLEMENTATION AND CONTINUOUS IMPROVEMENT

POLICY & PROCEDURE DEVELOPMENT: CREATE OR UPDATE SECURITY POLICIES, PROCEDURES, AND STANDARDS

AWARENESS & TRAINING: CONDUCT SECURITY AWARENESS SESSIONS FOR EMPLOYEES

RISK ASSESSMENTS & BUSINESS IMPACT ANALYSIS: INTERNAL RISK AND BIA ASSESSMENTS

INTERNAL AUDIT & READINESS: PREPARE SMT FOR INTERNAL AND EXTERNAL AUDITS

VS

GRC AS A SERVICE PROVIDER (EXTERNAL)

CORE SERVICES:

IMPLEMENTATION OF INTERNATIONAL STANDARDS & FRAMEWORKS: ISO 27001, ISO 22301,COBIT, ETC.

REGULATORY COMPLIANCE: GDPR, PCI DSS, SAMA, LOCAL LAWS

RISK & IMPACT ASSESSMENTS: RISK IDENTIFICATION, EVALUATION, MITIGATION, BIA, THIRD-PARTY RISK

ISO INTEGRATION: IMPLEMENTING AND INTEGRATING ISO STANDARDS (E.G., ISO 27001 WITH CBJ CYBERSECURITY FRAMEWORK OR ISO 22301).

CONSULTATION SERVICES: EXPERT GUIDANCE, GAP ANALYSIS, AND COMPLIANCE IMPROVEMENT FOR ISO 27001, GDPR, PCI DSS, ISO 22301.

SMT GRC SERVICES OVERVIEW

01
IMPLEMENTATION OF INTERNATIONAL STANDARDS & FRAMEWORKS

02
REGULATORY COMPLIANCE

03
RISK & IMPACT ASSESSMENTS

04
CONSULTATION & INTEGRATION SERVICES

IMPLEMENTATION OF INTERNATIONAL STANDARDS & FRAMEWORKS

01	ISO/IEC 27001:2022 – INFORMATION SECURITY MANAGEMENT SYSTEM	PROVIDES A SYSTEMATIC APPROACH TO MANAGING SENSITIVE INFORMATION THROUGH AN ISMS, ENSURING PROTECTION AGAINST CYBER THREATS AND COMPLIANCE WITH GLOBAL SECURITY STANDARDS
02	ISO 22301:2019 – BUSINESS CONTINUITY MANAGEMENTSYSTEM	SETS REQUIREMENTS FOR A BCMS THAT ENABLES ORGANIZATIONS TO RESPOND, RECOVER, AND MAINTAIN ESSENTIAL OPERATIONS DURING DISRUPTIONS OR CRISES.
03	ISO/IEC 20000-1 :2018– IT SERVICE MANAGEMENT	DEFINES BEST PRACTICES FOR IT SERVICE MANAGEMENT (ITSM), HELPING ORGANIZATIONS DELIVER RELIABLE, EFFICIENT, AND CONTINUALLY IMPROVED IT SERVICES
04	ISO/IEC 27701 – PRIVACY INFORMATION MANAGEMENT SYSTEM	AN EXTENSION TO ISO 27001, PROVIDING A FRAMEWORK FOR MANAGING PERSONAL DATA, ENHANCING PRIVACY PRACTICES, AND SUPPORTING COMPLIANCE WITH DATA PROTECTION LAWS SUCH
05	SOC 2 – SERVICE ORGANIZATION CONTROL IMPLEMENTATION	A FRAMEWORK FOR MANAGING AND SECURING CUSTOMER DATA BASED ON THE TRUST SERVICES CRITERIA: SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY.

IMPLEMENTATION OF INTERNATIONAL STANDARDS & FRAMEWORKS

06	ITIL – IT SERVICE BEST PRACTICES INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY	IMPLEMENTATION OF IT SERVICE MANAGEMENT BEST PRACTICES TO IMPROVE EFFICIENCY AND SERVICE DELIVERY
07	NIST CSF - CYBERSECURITY FRAMEWORK	IMPLEMENTATION OF A STRUCTURED APPROACH TO IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER FROM CYBER THREATS
08	COBIT IMPLEMENTATION CONTROLOBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY	IMPLEMENTATION OF IT GOVERNANCE AND MANAGEMENT PRACTICES TO ALIGN TECHNOLOGY WITH BUSINESS OBJECTIVES
09	PCI-DSS IMPLEMENTATION	IMPLEMENTATION OF SECURITY MEASURES TO PROTECT PAYMENT CARD DATA AND ENSURE COMPLIANCE WITH INDUSTRY STANDARDS
10	DATA CLASSIFICATION & PROTECTION	IMPLEMENTATION OF PROCCESSES TO CLASSIFY, SECURE AND MANAGE SENSITIVE DATA BASED ON ITS CRITICALITY AND CONFIDENTIALITY

REGULATORY COMPLIANCE

GDPR CONSULTATION & IMPLEMENTATION

SUPPORT ORGANIZATIONS IN COMPLYING WITH THE EU GENERAL DATA PROTECTION REGULATION TO PROTECT PERSONAL DATA AND PRIVACY

GDPR CONSULTATION & IMPLEMENTATION

ASSIST IN APPLYING CYBERSECURITY AND COMPLIANCE REQUIREMENTS SET BY THE CBJ FOR FINANCIAL INSTITUTIONS.

GDPR CONSULTATION & IMPLEMENTATION

IMPLEMENTATION OF CYBERSECURITY AND RISK MANAGEMENT FRAMEWORKS REQUIRED BY THE SAUDI CENTRAL BANK (SAMA), SUCH AS THE CYBERSECURITY FRAMEWORK (CSF) AND THE CYBER RESILIENCE FRAMEWORK (CRF).

GDPR CONSULTATION & IMPLEMENTATION

SUPPORT IN MEETING THE NATIONAL CYBERSECURITY AUTHORITY REGULATIONS IN SAUDI ARABIA TO ENHANCE CYBER RESILIENCE.

GDPR CONSULTATION & IMPLEMENTATION

NCSC
- CYBERSECURITY SERVICE PROVIDERS LICENSING FOR 2024
MINISTRY OF DIGITAL ECONOMY AND ENTREPRENEURSHIP
-PDPL

RISK & IMPACT ASSESSMENTS

BUSINESS IMPACT ASSESSMENT (BIA)

WE HELP ORGANIZATIONS IDENTIFY THEIR MOST CRITICAL BUSINESS FUNCTIONS AND EVALUATE THE IMPACT OF POTENTIAL DISRUPTIONS. THIS ENSURES BUSINESS CONTINUITY BY PRIORITIZING RESOURCES AND RECOVERY STRATEGIES.

PRIVACY IMPACT ASSESSMENT (PIA)

OUR EXPERTS ASSESS HOW PROJECTS, SYSTEMS, OR PROCESSES HANDLE PERSONAL DATA TO ENSURE COMPLIANCE WITH PRIVACY REGULATIONS. THIS MINIMIZES RISKS RELATED TO DATA MISUSE AND STRENGTHENS CUSTOMER TRUST

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

WE CONDUCT THOROUGH ASSESSMENTS TO EVALUATE POTENTIAL RISKS TO PERSONAL DATA, ESPECIALLY FOR HIGH-RISK PROCESSING ACTIVITIES

RISK & IMPACT ASSESSMENTS

CYBERSECURITY RISK AND MATURITY ASSESSMENT

WE EVALUATE THE ORGANIZATION'S CURRENT CYBERSECURITY POSTURE AND MATURITY LEVEL AGAINST INDUSTRY STANDARDS. THIS HELPS IDENTIFY GAPS, PRIORITIZE IMPROVEMENTS, AND BUILD A ROADMAP FOR STRONGER CYBER RESILIENCE

THIRD PARTY RISK ASSESSMENT

WE ASSESS THE RISKS ASSOCIATED WITH VENDORS, SUPPLIERS, AND BUSINESS PARTNERS TO ENSURE THEY MEET YOUR SECURITY AND COMPLIANCE REQUIREMENTS. THIS REDUCES EXPOSURE TO EXTERNAL THREATS

KEY RISK INDICATORS (KRIS) DEVELOPMENT

WE HELP ORGANIZATIONS DEVELOP MEASURABLE INDICATORS THAT TRACK AND MONITOR EMERGING RISKS IN REAL TIME. THIS ENABLES PROACTIVE RISK MANAGEMENT AND INFORMED DECISION-MAKING

CONSULTATION & INTEGRATION SERVICES

WE PROVIDE SPECIALIZED CONSULTATION AND SEAMLESS INTEGRATION SERVICES TO HELP ORGANIZATIONS ALIGN WITH INTERNATIONAL STANDARDS AND REGULATORY REQUIREMENTS

OUR SERVICES INCLUDE:

ISO INTEGRATION- ASSISTING ORGANIZATIONS IN IMPLEMENTING AND INTEGRATING ISO STANDARDS (E.G., ISO 27001 WITH CBJ CYBERSECURITY FRAMEWORK, OR ISO 27001 INTEGRATED WITH ISO 22301).

CONSULTATION SERVICES - WE PROVIDE EXPERT GUIDANCE, CONDUCT THOROUGH ASSESSMENTS, AND PERFORM GAP ANALYSES TO HELP ORGANIZATIONS IDENTIFY THEIR CURRENT COMPLIANCE STATUS AND AREAS FOR IMPROVEMENT. OUR SERVICES COVER STANDARDS AND REGULATIONS SUCH AS ISO/IEC 27001, GDPR, PCI DSS, AND ISO 22301.

DEPARTMENT CERTIFICATIONS

ISO/IEC 27001 LEAD IMPLEMENTER
ISO/IEC 27001 LEAD AUDITOR
ISO/IEC 27002 LEAD MANAGER
ISO/IEC 27032 LEAD CYBERSECURITY MANAGER
ISO/IEC 27701 LEAD IMPLEMENTER (PIMS)
ISO 22301 LEAD IMPLEMENTER (BUSINESS CONTINUITY)
CERTIFIED DATA PROTECTION OFFICER (DPO)
CERTIFIED TRAINER – PECB
CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA – ISACA)
ISO 27001 INTERNAL AUDITOR (QSCERT)
CERTIFIED IN CYBERSECURITY CC - ISC2
CERTIFIED ETHICAL HACKER - CEH
LEAD SOC2 ANALYST

GRC DEPARTMENT

GRC MANAGER

DANA MANSOUR

GRC TEAM

ANAS ABU IRSHAID

JALAL ARAFAT

LINA ABUKHALED

RAHAF ALBOJOQ

REFERENCES

CRIF
شركة المعلومات الائتمانية الأولى في الأردن

الديوان الملكي الهاشمي

مركز تكنولوجيا المعلومات الوطني
National Information Technology Center

وزارة الإتصالات و تكنولوجيا المعلومات
Ministry of Information and Communications Technology

ROYAL JORDANIAN
الملكية الأردنية
The way you want to fly

رؤيا

KPMG

REFERENCES


هيئة تنظيم قطاع الاتصالات
Telecommunications Regulatory Commission
1995


وزارة المالية
دائرة ضريبة الدخل والمبيعات


سلاح الجو الملكي


Ministry of Digital Economy
and Entrepreneurship


دائرة الأراضي والمساحة

REFERENCES

شركة الكهرباء الأردنية المساهمة العامة المحدودة
Jordan Electric Power Company

Classera®
True Joy of Smart Learning

EHS Electronic Health Solutions
Technology for better healthcare in Jordan

شركة توزيع الكهرباء المساهمة العامة
EDCO
ELECTRICITY DISTRIBUTION CO.

موضوع
www.mawdoo3.com

RSM

REFERENCES

مدفوعاتكم
MadfooatCom

مصرف الشمال
North Bank

ICS FS
ICS FINANCIAL SYSTEMS LTD

البوتاس العربية
Arab Potash

QUESTIONS?

THANK YOU