ebryx SECURENOW

# GRC CONSULTING SERVICES

**As the global regulatory environment continues to evolve, forcing changes across your organization, keeping up with various compliance standards and frameworks can become daunting and also exposes your organization to penalties related to non-compliances.**

Ebryx' Security Governance, Risk and Compliance (GRC) Services help organizations address the issues of corporate governance, enterprise risk management and compliance from the perspective of information technology and cybersecurity. We can help your organization identify, remediate, monitor, and manage enterprise IT security risk, facilitate decision making on organizational security strategy and help manage related costs. Our GRC team performs gap assessments against various cybersecurity frameworks and compliance standards to help you gauge the current state of your compliance with these standards and frameworks. For organisations looking to comply with any of the compliance standards we provide readiness services. Ebryx Security GRC services include the following:

- ISO 27001 Adoption, Implementation and Certification Readiness Service
- SOC-2 Gap Assessment and Readiness Service for Service Organizations
- HITRUST Gap Assessment & Compliance Readiness Service
- HIPAA Gap Assessment & Compliance Readiness Services
- PCI DSS Gap Assessment Services
- Information Security Risk Management Framework
- GDPR Compliance
- CCPA Gap Assessment & Compliance Readiness Service
- Business Continuity, Incident Response & Disaster Recovery Planning Services

With Ebryx' Security GRC Services your organization gets to:

- Identify and prioritize security threats and vulnerabilities
- Identify maturity level of existing security controls
- Enhance enterprise security policies, procedures and adopt best practices
- Meet mandatory compliance requirements
- Justify security investments
- Quickly establish trust with customers and other stakeholders

> 87% of organizations see tech risk management as a siloed, reactive process rather than "an organization-wide function for proactive risk management."
>
> KPMG / Forbes Insights, **Disruption Is the New Norm: Tech Risk Management Survey Report**, 2018

## ISO 27001:2013 Adoption, Implementation and Certification Readiness Service

### Introduction

ISO 27001 (ISO/IEC 27001:2013) is the international standard that provides the specifications for an information security management system (ISMS).

The standard is designed to help organizations manage their information security processes in accordance with international best practices while optimizing costs. It is a technology- and vendor-neutral standard and is applicable to all organizations irrespective of their size or nature.

## ISO 27001:2013 Gap Assessment and Readiness Service

An ISO 27001 gap analysis provides a high-level overview and analysis of requirements to be fulfilled to achieve compliance and certification. This gap analysis also exhibits the organization's existing compliance posture against the requirements of ISO 27001. Being compliant with ISO 27001 enables organizations to provide information security assurance to its key stakeholders. Being ISO 27001 compliant reduces the likelihood and impact of critical data breaches.

Ebryx provides a pathway to implement people-based, process-based and technological controls in your organization to fill information security gaps. This exercise enables organizations to build a robust and tailored Information Security Management System (ISMS) to cater to their information security needs. Our methodical approach enables organizations to obtain and maintain ISO 27001 certification easily and quickly. Our ISO 27001 Gap Analysis Service is coupled with Vulnerability Assessment Service, Penetration Testing Service, Security Operations Center (SOC) Services and ISO 27001 Internal Audit services. These services enable you to go beyond gap identification to the actual implementation of the various security measures required by the standard.

## System and Organizations Controls (SOC-2) Gap Assessment and Readiness Service for Service Organizations

SOC-2 (AICPA) is a report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy. Regarding your organization, the audience of SOC-2 reports is a large range of stakeholders that need detailed information and assurance about the controls your organization has deployed relevant to security, availability and processing integrity of the systems.

These reports ensure the implementation of the following:

- Active Organizational and Regulatory oversight over the organization
- Vendor Management System
- Corporate Governance Framework and Risk Management Regime

SOC-2 reports highlight the management's description of a service organization's system and the suitability of the design of controls.

For SOC-2 readiness, Ebryx works with key stakeholders across business and IT groups to identify and understand the full set of drivers and potential uses of the SOC 2 report. This includes a thorough review of policies, procedures, internal controls and business processes. Location of critical customer data and supporting system functionality is also considered to create a comprehensive map of the "in-scope" IT environment. Ebryx provides process and policy level design and drafting support to adopt SOC-2 requirements. Along with this, Ebryx provides Vulnerability Assessment Services, Penetration Testing Services, Security Operations Center (SOC) Services that fulfil key requirements of SOC-2.

> "Cybersecurity and data protection is a top area of concern, with 70% of chief audit executives ranking cyber risk as high or very high at their organizations."
>
> Institute of Internal Auditors (IIA), **North American Pulse of Internal Audit: Defining Alignment in a Dynamic Risk Landscape**, 2019

## HITRUST Gap Assessment & Compliance Readiness Service

HITRUST stands for the Health Information Trust Alliance. The HITRUST approach is a systematic methodology that helps organizations from all sectors, especially the healthcare sector, to effectively manage their data, cater to information security risks and maintain sector-specific compliance. HITRUST certification by the HITRUST Alliance enables vendors and covered entities to demonstrate compliance to HIPAA requirements based on a standardized framework.

Ebryx provides HITRUST adoption services by providing policy and process level design and document support. This service is complemented by Ebryx Vulnerability Assessment Services, Penetration Testing Services and Security Operations Center (SOC) Services.

## HIPAA Gap Assessment & Compliance Readiness Services

HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States law that mandates the adoption of a mechanism for data privacy and security for safeguarding medical information. The HIPAA Privacy and Security Rules provide safeguards for Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) held or transmitted by a covered entity or business associate.

Ebryx offers a complete range of services to help organizations and covered entities in complying with the HIPAA security requirements. We have extensive expertise in logical, physical and administrative controls deployment that can be highly effective to achieve HIPAA compliance. Our Security Services are directly aligned with many components of the HIPAA Security Standards which reduces the cost to conform to the HIPAA requirements.

## PCI DSS Gap Assessment Services

The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.

PCI DSS gap assessment is performed in the early phases of PCI compliance adoption. This enables an organization to quickly identify gaps regarding PCI DSS requirements based on which a remediation plan can be crafted in which the required effort and actions are estimated to reach a compliant state.

For gap assessment, Ebryx performs a thorough on-site and off-site review of systems, policies, processes and procedures with staff members along with a documentation review.

Following are some key outcomes of PCI Gap Assessment:

- Organization's current state of PCI DSS compliance
- Identification of gaps that need to be prioritized and remediated
- PCI compliance cost forecasting and budgeting justification and recommendations
- Detailed recommendations for gap remediation

> “Over 75% of executives report that their organizations either have no method to measure cyber risk (49%) or they don't know if their organization measures risk exposure (27%).”
>
> Marsh & McLennan Agency, **Managing Cybersecurity: The Cyber Risk Perception Survey**, 2018

## Information Security Risk Management Framework

Information security risk management frameworks help organizations to identify and assess threats and vulnerabilities and implement key security controls in their organizational and technological environment.

Risk Management is a key area of any information security framework which drives all organizational efforts to systematically sort out security goals. Organizations with optimized and fully functional risk management systems realize greater benefits as compared to those having no or dysfunctional risk management systems.

Various information security standards, laws and frameworks require organizations to have their own Risk Management

Frameworks. Such frameworks include NIST, ISO 27001 etc. Ebryx helps organizations to design, implement, manage and improve their risk management frameworks that comply with the requirements of information security laws and frameworks.

## GDPR Compliance (Website, Application Compliance & Organizational Compliance)

The General Data Protection Regulation (GDPR) is a regulation for European countries on data protection and privacy. GDPR primarily aims to give control to individuals over their personal data.

GDPR regulation is enacted in a way that it applies virtually to every organization which is offering its goods or services to Europe or is handling personal identifiable information of EU citizens. In such cases, it becomes immaterial whether these organizations are located inside or outside the EU. In certain situations GDPR requires compliant organizations to appoint a Data Protection Officer to oversee the compliance activities.

Ebryx provides a complete range of GDPR compliance services including application (software) architecture compliance, website architecture compliance and organizational compliance. In certain cases where organizations require Data Protection Officer's services, Ebryx provides Data Protection Officer's services thus helping your organization to meet the compliance requirements.

## CCPA Gap Assessment & Compliance Readiness Service

California Consumer Privacy Act 2018 is the law passed by the State of California as a response to the increased role of personal data in contemporary business practices and the personal privacy implications surrounding the collection, use and protection of personal information. Failure to comply with CCPA puts organizations at risk of huge fines.

Ebryx provides full spectrum CCPA compliance assessment and readiness services to assist organizations in meeting the CCPA compliance requirements, to protect personal data as well as honor consumers' rights as per CCPA. Our service includes the identification of any potential gaps between the practices and CCPA requirements and proposing corrective actions to be taken in order to bridge any CCPA compliance gaps.

## Business Continuity, Incident Response & Disaster Recovery Planning Services

Good business continuity strategies keep your company up and running through major disruptions like natural disasters, system hacks, power failures, vendors unavailability etc. Business Continuity and Disaster Recovery planning enables organizations to prepare for disruptive and unfavorable events.

Ebryx provides a wide range of Business Continuity and Disaster Recovery services including Business Impact Analysis (BIA), preparation of BC & DR plans and playbooks, execution of BC & DR mockups and drills to test the effectiveness of plans in an emergency.

## About Ebryx

**Ebryx is a leading cybersecurity, software and hardware solutions company with vast experience in security product engineering, malware research and managed and consulting services for customers around the world. Our team of security analysts and consultants is well-equipped through renowned industry certifications like GIAC Reverse Engineering Malware (GREM), GIAC Certified Forensic Examiner (GCFE), GIAC Certified Intrusion Analyst (GCIA), Offensive Security Certified Professional (OSCP) and Certified Information Systems Security Professional CISSP.**