

BRS INFORMATION SECURITY MANAGEMENT SYSTEM, ISMS



SECURITY WITHIN THE ENTERPRISE ENVIRONMENT

BRS ISMS Covers:

- Protection of data and information,
- Network and usage,
- E-mail clients,
- Voic Mail,
- Workstations,
- Remote access,
- Portability of information,
- Contractors, and
- Other specifics agreed

By identifying threats and qualifying these as aspects of risk, can determine and act with appropriate controls. This protocol from identification through implementation of controls are to preserve confidentiality and at the same provides for portability of information,

Corporate accountability, regulatory compliance and legal risk management are only a few of the driving force for ISMS. BRS ISMS is based on ISO/IEC 27001 and suitable for today's enterprise. ISO/IEC 27001 provides best practices for security of information. ISO/IEC 27001 certification allows organizations to establish, implement and maintain an effective Information Security System that address current and future regulations sustainable and effectively, ISO/IEC 27002.

Effectiveness in succeeding and improving information security requires a "secure" enterprise relying not in just monitoring its parts, but proactively managing the

network and assets as a whole.

ISMS is more than just compliance and security—is about establishing the fundamentals to face the challenges of information and technology to achieve conformity and certification to sustain regulations and legal obligations.

Through check and balances, BRS ISMSA (Information Security Management System Assessment) provides a "holistic" approach to analyze and identify actions contributing before they can wreak havoc; and objectively demonstrate to others your organization's commitment, competence and capability for security of information (and its assets).

TECHNOLOGY, INNOVATION...

In today enterprise technology speed and efficiency are imperative, but the real benefit resides when is use to act differently or in providing us with a path of doing things that were not possible before, to innovate.

ISMS propitiates the fundamentals for a secure physical and virtual environment , whether small, medium or multinational enterprise and a means to innovate.

What is BRS IS.MS

Initiating toward BRS IS.MS

What follows

Frequently asked questions, FAQ

Some of the benefits that ISMS ISO/IEC 27001 provides:

- Basis for regulatory and legal compliance
- Corporate accountability
- Reduce legal risk
- Maintaining access to information
- Maintaining and improving productivity
- Improved decision-making, by the availability and access of information
- Business Continuity
- Compatible with other information security management systems such as COBIT

WHAT IS ISMS ISO/IEC 27001 CHALLENGE...

ISMS fundamentals reside in the implementation of benchmarks ISO/IEC 27002, and assess through ISO/IEC 27001 to achieve certification status. ISO/IEC 27001 can either be a stand alone or part of Adding-Value-Assessment with ISO 9001, ISO 14001 or ISO 22000 management systems certificate of registration protocol.

To achieve ISMS an organization's information security management system requires adherence to ISMS Assessment Verification (ISMSA) check sheets. ISMSA ISO/IEC 27001 provides the criteria against assessing an organization's ISMS provides for 3rd

party assessment and granting of a certificate resulting in confidence and assurance that the certification holder has implemented, maintains, updates and improves security activities through a system that manages information security requirements. HIPAA, Visa CISP/PCI, FACT, GLBA, California SB-1386 and derivatives from Basel II, EU Directives on the Protection of Personal Data as well Canadian Personal Information Protection and Electronics Documents Act (PIPEDA) are just a few regulations. ISMS intent is to instill accountability and governance controlling and

minimizing security breaches. Market confidence and conditions continue creating threats as well the evolution of regulatory compliance create enormous challenges. Cybercrime is becoming the profitable choice for ill intent and organizational security vulnerability from malicious intent.

BRS ISMSA—Information Security Management System Assessment is the BRS guiding basis for BRS ISMS verification either as standard alone or integral to QMS ISO 9001, MDD ISO 13485, or FSMS HACCP MS and ISO 22000.

...constant innovation, update and to improve the operating environment... optimizing processes...

BRS ISMSA comprises of 3 parts:

Part I—Initial information gathering and introduction to client-organization.

Part II—ISMSA team information gathering for policies assessment and planning.

Part III—The ISMSA specification check sheets. This is for the BRS ISMS team to assess, evaluate and conclude on the effectiveness of safeguarding information.

YOUR BUSINESS AND TECHNOLOGY

Technology is a means to an end, and the end is success through profitability and growth, and the way to get there is by doing what your organization does best... and this means that constant innovation and improving the operating environment, and it means optimiz-

ing processes, these are needs of the contemporary enterprise.

Your organization has established and maintains a barrage of software and hardware and continuously strives for best protection. And ISMS, by relentlessly striving to become #1 solu-

tion provider for managing security of information, provides best true protection.

ISMS propitiates a fundamental management system as a basis for benchmarking and thereon improving the environment wherein information security resides.

INITIATING, Phase I

Phase I (see also implementation thoughts, page 3) – After implementation of ISO/IEC 27001 | ISO/IEC 27002 integral to your organizations process and activities, ISMS certified security team assessors evaluate policies for security,

referring to level I documents. It is expected that the organization demonstrate competence in effectively managing security and maintenance protocols.

After acceptance of quote, inquire on the complete BRS ISMS Assessment Document (ISMSA) Part I, II and III— which is available to client-organizations.

WHAT FOLLOWS, Phase II?

The on-site assessment, with the organizations permission—authority and witnessing can include a system tests to verify vulnerabilities and threats.



Phase II – On-site assessment by a BRS ISMS professional assessment-auditor to verify the management system implementation through; evaluations, tests, following trails, observations, and interviews seeking evidence that demonstrates effectively conforming to the ISMS specifications. The BRS on-site assessment includes the sites’ physical security measures.

The assessment team concludes with evidence and information obtained, and through a recommendation determining the organization conformance to ISMS and legal obligations. Findings may require corrective action need be address prior to proceeding to recommendation to a panel of independent

and competent BRS designees for concurrence as these are relevant to risk and vulnerabilities threats that need be assessed prior to the concurrence of recommendation, as these are part of fulfilling the requirements within BRS ISMSA (ISO/IEC 27002 | ISO/IEC 27001). After the concurrence of recommendation then proceed to the registration in adherence to legal compliance.

Phase III - After awarding the certificate of registration, every 6 to 9 months continuing assessment protocol through the BRS certified assessors and proceeding to recommend to the BRS Quorum of the Regions and to have available for the Global-Net Oversight Board ac-

creditation assessments. After issuing BRS ISMS certification it is require that the organization maintains fulfilling the requirements of ISMSA (ISO/IEC 27002 | ISO/IEC 27001) and improving. ISMSA applies to BRS “Autonomation Assessments”.

At the end of the 3-year period a re assessment of the organization BRS ISMS is require for continuance of certification.

* BRS delegates review the recommendation which comprises from competent exclusive professionals from around the world.

Implementation thoughts, Phase I...

BRS ISMS specific requirements apply ISO/IEC 17799 | ISO/IEC 27002 based BRS ISMSA as guidelines plus BRS added specifications for the organization to establish, implement, maintain and improve within the realm of information security.

Note: BRS assessment will verify whether the organization conforms to the requirements of BRS ISMSA which is not uniquely ISO/IEC 27001 but also additional requirements agreed with the organization.

Upon implementation of BRS ISMSA it is require that the security policies and management practices remain operational for a period of time prior to the certification assessment (BRS requires a minimum of 3 months). This time period ensures that the implementation is effective to the policy and objectives set forth in addressing BRS ISMS specifications (BRS ISMSA). Once assessing the organization’s management system by competent internal personnel and management reviews effectiveness of implementation then your organization most likely ready for the BRS ISMSA Assessment.

While ISMS is not all IT, today's IT Professional needs becoming part policy maker and enforcer, all while interacting with legal requirements when creating an effective IT effectively-use policy, practices and methods. BRS ISMS is an 3rd Party validation of best and effective practices. ISMS is about business continuity...



GUIDING DOCUMENTS FOR BRS IS.MS CERTIFICATION - REGISTRATION

Benchmark Specifications for Certification

- ISO/IEC 27001 Information Security Management Systems, ISMS – Specification with Guidance for use + references from ISO 9001:2000 Quality Management Systems – Requirements (e.g. 6.3, 6.4, 7.2, 7.4... Section 8)
- ISO/IEC 27001—Specification for Information Security Management
- ISO/IEC 27001 implementation based ISO/IEC 27002 based BRS ISMSA applies as a specification-guiding document, not as purely specified document.

ISO/IEC 27006 Accreditation assessment protocol

- ISO/IEC 27006 is the guidelines on combined management systems auditing under accreditation.

Other documents as relate to guidance and applicable to BRS

- Benchmark ISO/IEC 17021 and ISO 19011 for accredited certification bodies
- EA 7/03, Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems.

The ISMS Assessment Team

BRS has lead the way in training professionals in Europe in ISMS ISO/IEC 27001... we qualify and certify our own of professionals based on methodologies concurrent international recognized benchmark ISO/IEC 17024 accreditation. The BRS assessment team includes two the following competencies and qualifications:

- ISMS Assessors
- IS Specialist, as the agreement determines

BRS ISMS USA accredited certification is approved and recognized in the European Union as well internationally. The BRS process provides a competent Assessment Team requiring technical and communication skills, training, knowledge, education and experience in security networking, hardware, software, firmware, and management system.



The BRS ISMS assessment team, in our  effort, brings a little extra to meet and exceed client expectations: The team is knowledgeable in a number of technology advances involving Windows, Linux, Unix , Sun Solaris, BSD, IRIX, Mac OS platforms. And applications and environments within industry sectors as mining, petroleum, manufacturing, service (CRM), ERP, CAD/CAM, PSpice... over hardware and firmware from Cisco Networking (security), Cray, DEC-Alpha, Sun-Ultra, NCR, VA... Further, AI, cyber-criminal activities, hacking techniques, technology forensics... an arsenal to assist in ascertaining that BRS IS.MS creates the basis to achieve true IS.

“...Cisco Networking security, IT, PSpice, CRM, ERP, Unix, Windows, Linux, AI...”

Answering Questions, FAQs

BRS ISMSA and ISO/IEC 27002 | ISO/IEC 27001? These are intended to...

...facilitate interacting with other management system standards, such as ISO 9001 for quality management, ISO 14001 for eco-management and ISO 22000 for food safety, and others including ISO 13485 for regulatory compliance.

BRS ISMS includes implicit requirement for continual improvement of concurrent principles with ISO 22000, ISO 9001 and ISO 14001 and other variants. Through the “Plan, Do, Check and Act” process model inclusive to the management system approach for developing, implementing, and improving the effectiveness of an organization's information security management system (ISMS).

ISO/IEC 27002 informative Annex

Interacting controls (Section 4) ISO/IEC 27002 | Interaction with ISO/IEC 27001—BRS ISMSA...

Controls set forth by example Section 4 of BS 7799 Part 2 directly derived from and aligned with those in ISO/IEC 27002 and ISMSA. The control objectives and controls are contained within Annex A. BRS applies these as guides and adds specifications based on the knowledge and experience of the BRS Core Team—Quorum of the Regions.

We have implemented ISO 9001; can we combine with ISO/IEC 27002 | ISO/IEC 27001 and integrate both management systems?

Yes, as example; ISO/IEC 27001 provides for explanations how management system standards relate. Combining management systems assist in reducing the maintaining effort and thus avoiding dual standards and double work. Dependent on the requirements that your organization must meet, each management certifications requires its own considerations. Further, consideration needs be given to the complexity of your business activities.

What is BRS ISMS stand alone and complementary to other standards... and Accreditation?

BRS while operating under USA and EA Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems (ISMS) EA 7/03, is consider for mainly providing ISMS within ISO 9001, ISO 14001, and ISO 22000, and can achieve stand alone ISMS. One of reasons being is that BRS provides ISMSA | ISMS to registered client organizations.

Accreditation provides confidence in ISMS certification. As a USA based Certification Body we are one of the few worldwide that benchmarks ISO/IEC 27006 Accreditation.

Why are the ISMS ISO/IEC 27001 and ISO/IEC 17799—27002 schemes important?

Organizations are implementing and certifying for numerous reasons, among these; CRM business process, e-business activities, requirements set forth in compliance with and relevant to “Data Protection Act”, corporate directives (alliance or partnerships), GLBA, HIPAA, CFR 21 Part 11, Sarbanes-Oxley... requiring that the business information security is protected through 3rd party assessment and certification is achievable to maintain regulatory mandates.

Does ISO/IEC 27002 | ISO/IEC 27001 recommends a specific risk assessment methodology?

No, ISO/IEC 27002, ISO/IEC 27001 nor BRS ISMS / ISMSA while requiring that the organization performs risk assessment do not invoke any specific methodology. Risk is the basis upon which the ISMS flows through planning, development, implementation, maintenance and continual improvement.



ISMS ISO / IEC 27001

North America

Europe

Euro Asia

Latin America

Asia Pacific

Middle East

Rim of the World Office
31977 Hilltop Suite D at PO BOX 1020
Running Springs, California USA 92382

Voice center—1.909.867.4003
TEL 909.867.4003

Inquire, after your organization acceptance of quote, for the complete BRS ISMS Assessment Document—available to client-organizations. Prior apply ISO/IEC 27002 and ISO/IEC 27001, as BRS ISMS is based on guidance of these international standard.

IN CONCLUSION:

We realize that the business driver for ISMS ISO/IEC 27001 is the need to a pragmatic approach in going forward to establish-implement-maintain-update-improve to address regulatory and legal compliance for the protection of consumers and communities as a legally binding charter, and to do so effectively and efficiently.

Similar—Facsimile of Certificate of Registration CoR...

