Monetize your Critical Data Asset

Simplified Integration as a Service [SiaaS]SM

Quality Manual

Quality & Information Security Management System

(IMS) Manual

(ISO9001:2015 & ISO27001:2013)

Issue:01

Dated: January 2nd, 2022

Revision History

Serial Number	Date MM/DD/YY	Details of Change	Page Numbers	Revision Number
1	09/20/2021	Initial Draft	All	1.0.0
2	01/02/2022	Initial Release	All	1.0.0

Audit History

Serial Number	Date MM/DD/YY	Details	Auditor	NCR Count

Authorization

Prepared by	Role: VP Operations	Signature on file	Date 01/02/2022
Reviewed by	Role: VP Business Development	Signature on file	Date 01/02/2022
Approved by	Role: President	Signature on file	Date 01/02/2022

Table of Contents

1 Introduction

This section presents the Scope of the Information Security Management System (ISMS). This includes the purpose and the application of ISMS.

1.1 Scope

The Scope of the IMS covers, the accel bi, its PMO office and its management related to business applications, to implement the IT services, Staffing services & project management provided to internal and external customers from its office location at 2406, 185 Place, Northeast, Redmond, WA 98052.

(Note: refer to Latest version of **'QMSPLAN20 SOA**.xlsx**'** for exclusions)

As per ISO9001:2015 requirements of clause 8.3 Product Design & Development are not applicable to accel bi as, we are providing services to customer as per customer specifications & guidelines mentioned in contract agreements.

1.2 General

This IMS manual specifies the requirements for establishing, implementing, monitoring, reviewing, maintaining, and improving documented IMS within the context of the overall Business requirements. It specifies the implementation of security controls customized to the needs of accel bi

The IMS is designed to ensure adequate and appropriate security controls that maintain Confidentiality, Integrity, and Availability (CIA) of information assets.

For applicability (with rationale) and exclusion (with justification) of controls refer Statement of Applicability (SOA). The SOA as applicable to accel bi is enclosed. As certain controls are not applicable.

1.3 References

The following documents were referred for the creation of this document. These include:

- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements
- ISO9001:2015 Requirements for Quality management system
- ISO19011:2018 Auditing Guidelines

1.4 Terms, Definitions, Acronyms, and Abbreviations

ABBREVIATION	DESCRIPTION
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity and Availability
CISO	Chief Information Security Officer
DB	Database
DP	Departmental Procedure
DR	Disaster Recovery
ED	Executive Director
HOD	Head of Department
HQ	Head Quarter
HR	Human Resource
IPR	Intellectual Property Right

ABBREVIATION	DESCRIPTION
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSC	Information System Security Committee
IT	Information Technology
NC	Non Conformity
NDA	Non-Disclosure Agreement
RA	Risk Assessment
RTP	Risk Treatment Plan
SOA	Statement of Applicability
SP	Standard Procedures
TSX	Technical Services Department
VA	Vulnerability Assessment
IMS	Integrated management System

TERMS	DESCRIPTION
Asset	Anything that has a value to the organization.
Availability	The property of being accessible and useable upon demand by an authorized entity
Business Continuity Plan (BCP)	A plan to build-in proper redundancies and avoid contingencies to ensure continuity of Business
Computer Media	Includes all devices that can electronically store information. This includes but not limited to diskettes, CD's, tapes, cartridges, and portable hard disks.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Continual Improvement	Continual Improvement refers to stage improvement programs that facilitate rapid improvement phases with intermediate stabilized phases.
Control	A mechanism or procedure implemented to satisfy a control objective
Control Objective	A statement of intent with respect to a domain over some aspects of an organization's resources or processes. In terms of a management system, control objectives provide a framework for developing a strategy for fulfilling a set of security requirements.
Disaster Recovery (DR)	A plan for the early recovery of Business operations in the event of an incident that prevents normal operation
Fallback	Provisions to provide service in the event of failure of computing or communications facilities.
Information Security	Security preservation of Confidentiality, Integrity and Availability of Information

TERMS	DESCRIPTION
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be involved
Information Security Incident	A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Security Management System (ISMS)	That part of overall management system based on business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Organization	Refers to accel bi unless specified otherwise.
Risk	The combination of the probability of an event and its consequence
Residual Risk	The risk remaining after risk treatment.
Risk Acceptance	Decision to accept risk
Risk Analysis	Systematic use of information to identify sources and to estimate the risk.
Risk Assessment	Overall process of risk analysis and risk evaluation
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Management	Coordinated activities to direct and control an organization with regard to risk.
Risk Treatment	Process of selection and implementation of measures to modify risk
Statement of Applicability	Document describing the control objectives and controls that are relevant and applicable to accel bi, IMS based on the results and conclusions of the Risk Assessment and Risk Treatment Processes. It should clearly indicate exclusions with appropriate reasons.

2 About the Manual

This section presents a brief overview of the Quality & Information Security Management System (IMS) manual of accel bi

2.1 Organization of the Manual

The IMS manual is intended as a reference document describing the security framework adopted by accel bi. It is organized as per the Table of Contents.

2.2 Document Availability

This document is available to all employees of the accel bi internal webpage https://www.accelbi.com/QMS

This is a read-only copy and the relevant part of the documentation is available to only authorized users based on their business requirements.

2.3 Document Control Information

It is the responsibility of the accel bi to release an approved document for the accel bi.

3 Organization Overview

This section presents an overview of the accel bi and its operations.

3.1 Mission Statement

'accel bi's mission is to fulfill the promise of applying technology to enable the success of customer business by performing at a level of trust, partnership, and innovation that far exceed what customers have come to expect from accel bi. In the same way, we know that we must exceed what our professionals have come to expect from employers to achieve that aspiration.

Mission Statement: Deliver capabilities that genuinely matter for business agility by becoming a mature champion goto partner for our customers, business associates, and employees.

4 Context of the Organization

4.1 Understanding the Organization and it's Context

accel bi shall determine external and internal issues that are relevant for delivering the services and Business Operation that affect its ability to achieve the intended results of ISMS. The issues which are considered necessary for delivering the services to internal and external stakeholders are given in the SWOT analysis.

Refer:QMO220 SWOT Analysis

4.2 Understanding the Needs and Expectation from Interested Parties

accel bi shall determine the following:

a) Interested parties that are relevant to IMS- All customers (Internal and External), Vendors, Supporting the Infrastructure & other Business operation, All employees providing & getting services for Business operation.

b) The requirement of these interested parties relevant to Information Security, the needs and expectations from external as well as internal customers are considered as under, and will be reviewed and updated over a period of time as part of continual improvement.

Table 4.2 Needs & expectation of interested Parties

Internal	Interested Party	Needs of Expectations
	Management	Compliance with Company Polices & timely response
	Employees	Employee Development & growth
	Shareholders	Return on investment & Reputation
	Board of Directors	Return on investment & Reputation
	Users / Other departments	Conductive Work environment
External	Interested Party	Issues
	Customers	Timely Delivery, No errors
	Vendors	Consistent Business & log term association
	Government	Compliance with applicable requirements
	Society and environment	Employment Opportunities

4.3 Determining the scope of the Information security management System

The Scope of the IMS covers,

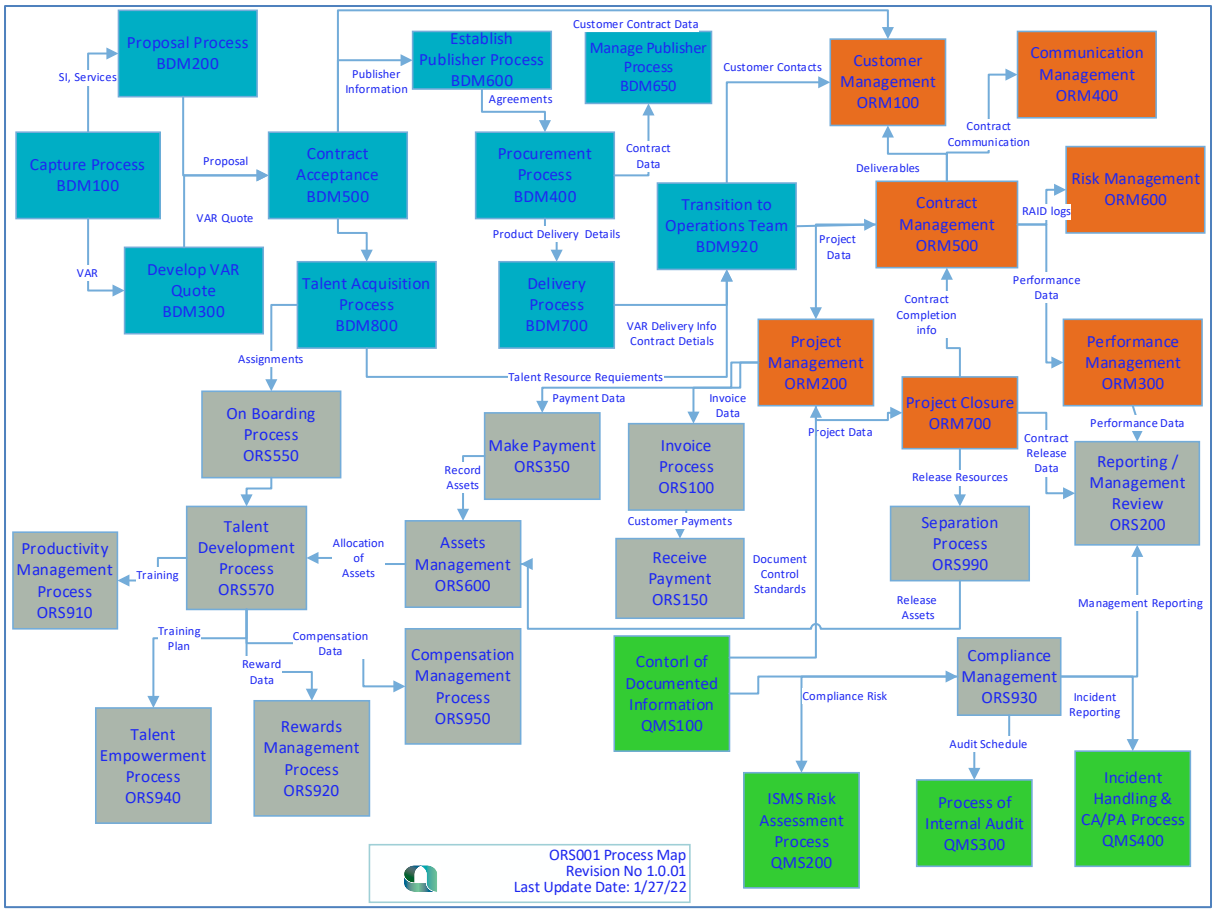
- Issues listed SWOT Analysis are considered
- Needs & expectation of interested Parties as listed in above table (**Table 4.2**)
- Interface & dependencies performed by accel bi & those that are performed by other organizations referred in **Fig 4.4**
- Boundaries of IMS are Business operations performed form accel bi at 2406, 185 Place, Northeast, Redmond, WA 98052

Note: refer to SOA for exclusions – "QMSPLAN20 SOA"

4.4 Information Security Management System

ACCEL BI has established, implemented, Maintained IMS and continually improving an Quality and Quality & Information security management system, in accordance with the requirements of ISO9001:2015 & ISO 27001:2013.

Fig 4.4 Process Interactions



Core Process

- BDM200 Proposal Process
- BDM500 Contract Acceptance
- ORM500 Contract Management
- ORM200 Project Management
- ORS570 Talent Development Process
- ORM300 Performance Management

Supporting Process

- BDM400 Procurement Process
- BDM800 Talent Acquisition Process
- ORS200 Reporting and Management Review
- ORS930 Compliance Management

Outsourced Process

- QMS300 Process of Internal Audit
- ORS950 Compensation Management Process
- Legal Services

5 Leadership

This section presents the accel bi's initiative and commitment to effective implementation and operation of IMS. In addition, this section highlights the roles and responsibilities associated with IMS operation.

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the Quality & information Security management system by:

A. Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.

B. Ensuring the integration of the Quality & information security management system requirements into the organization's processes.

C. Ensuring that the resources needed for the Quality & information security management system are available.

D. Communicating the importance of effective information security management and of conforming to the Quality & information security management system requirements.

E. Ensuring that the Quality & information security management system achieves its intended outcome(s);

F. Directing and supporting persons to contribute to the effectiveness of the Quality & information security management system.

G. Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

H. Please refer to ORM920 Compliance Management.

5.2 IMS Policy

accel bi's Information Security Policy commits the company to protect the security of its Information. It provides the same commitment to information entrusted to accel bi by its customers and business partners.

accel bi has established Quality & information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives or provides the framework for setting Quality & information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the Quality & information security management system.

The information security policy is:

a) available as documented information;

b) communicated within the organization displaying on intranet.

c) available to interested parties by putting it on the company website

ISMS Policy

We at accel bi committed to maintain high quality standards in delivering timely and cost-effective solutions to our customers by

a) Continual improvement of our processes,

b) instilling quality consciousness amongst all employees,

c) Satisfying applicable requirements related to Information security.

d) Recognizing the confidentiality, integrity and availability of information assets to relevant stakeholders including our customers.

Date: 9/10/2021 Vice President (Business Development):

Quality Policy

We at accel bi are committed to deliver on time Quality Products & Services that comply with requirements of internal as well as external interested parties including applicable statutory and regulatory requirements. We shall achieve this by:

a) Continually improving efficiency & effectiveness of all processes.

b) Reducing variation and waste in the processes

c) Ensuring focus on risk and opportunities that can affect the quality of our products & services while striving to become a world-class organization.

Date: 9/10/2021 Vice President (Business Development)

5.3 Organizational Roles, Responsibilities & Authority for Information Security

accel bi is committed to Information security. The management has constituted Quality & Information System Security Committee, which is responsible for defining and improving the IMS. Management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the IMS as defined in IMS documentation, by

A. Establishing an Quality & information security policy;

B. Ensuring that information security objectives and plans are established;

C. Establishing roles and responsibilities for Quality & information security;

D. Communicating to the organization the importance of meeting Quality & information security objectives and conforming to the Quality & information security policy, its responsibilities under the law and the need for continual improvement;

E. Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the IMS;

F. Deciding the criteria for accepting risks and the acceptable level of risk;

G. Ensuring that internal IMS audits are conducted;

H. Conducting management reviews of the IMS.

IMS Team Role:

The Information Security Committee/team will meet once every month, support and supervise the activities of the accel bi, taking informed decisions. It will be held responsible for achieving measurable progress.

IMS Team Responsibility & Authority:

Review, test and reassess the strategy plan to determine the overall approach to business continuity. Responsible for reviewing security incidents and vulnerabilities and decide action to be taken on them.

A. Identify and define plans to protect critical business process from the major failure of information system or disasters and to ensure timely resumptions of business activity

B. Review, test and reassess the strategy plan to determine the overall approach to business continuity.

C. Responsible for reviewing security incidents and vulnerabilities and decide action to be taken on them

D. Carry out RA and prepare RTP

In addition, the group helps reduce the risk of disruption of business operation by providing advice on all aspects of security including:

A. Security Awareness

B. Data Confidentiality and Privacy

C. Logical Access

D. Data Communications

E. Systems and Data Integrity

F. Physical Security

G. Personal and Procedural Controls

H. Contingency and Disaster Recovery Planning

EMPLOYEES: Expected to follow security policy, processes, and procedures as documented in ISMS. Refer: Organization Structure & Role, responsibility & Authority document "ABIOrgCht-V1.02"

6 Planning

Actions to address risks and opportunities

6.1 General

When planning for the Quality & information security management system, accel bi shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) Ensure the Quality & information security management system can achieve its intended outcome(s);

b) Prevent or reduce, undesired effects; and

c) Achieve continual improvement.

accel bi shall plan:

a) Actions to address these risks and opportunities; and

b) How to

1. Integrate and implement the actions into its Quality & information security management system processes; and

2. Evaluate the effectiveness of these actions.

Refer: IMS Risk Assessment sheet QMO210 Information Security Risk Log"

6.1.1 Information security risk assessment

accel bi shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1. the risk acceptance criteria; and

2. criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

2. identify the risk owners;

d) analyses the information security risks:

1. assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2. assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3. determine the levels of risk;

e) evaluates the information security risks:

1. compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2. Prioritize the analyzed risks for risk treatment.

accel bi shall retain documented information about the information security risk assessment process. Risk management will be done as per 'accel bi-Risk Assessment & Risk Treatment Procedure QMS200' and the risk will be evaluated based on asset value, threat, vulnerabilities and possibility of occurrence. If risk value is high, adequate controls will be implemented.

Action Guideline:

a) accel bi prevents leakage, destruction, and illegal use of all information relating to the customers, vendors, management, products, technology developed & used etc. and builds the system to secure the confidentiality, integrity and availability of the information for daily operations.

b) Company recognizes the value of the private information of all staff and secures it.

c) accel bi establishes a contingency plan QSPLAN10 to secure continuation of the business, assuming occurrences of a natural disaster, terrorism, a large scale infection disease, fire etc.

d) Company provides all staff with proper education and training to maintain and improve the effectiveness of the information security management system

e) Company builds and manages an organization which grasps incidents, audits its operations and effectiveness of the information security management system, and attempts its continuous improvement.

To secure its information assets and it's customer, accel bi shall deploy procedures to maintain confidentiality, integrity and availability of all information assets.

6.1.2 Information security risk treatment

accel bi shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE: accel bi can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A of the standard ISO 27001:2013 and verify that no necessary controls have been omitted;

NOTE 1 Annex A of the standard ISO 27001:2013 contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A of the standard ISO 27001:2013 to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A of the standard ISO 27001:2013 are not exhaustive and additional control objectives and controls may be needed.

d) Produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) Formulate an information security risk treatment plan; and

f) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. accel bi retain documented information about the information security risk treatment process.

The details of the RA process can be referred from 'PROCEDURE FOR RISK ASSESSMENT AND TREATMENT QMS200'. The outputs of the RA process include:

- Risk Assessment Report
- Risk Treatment Plan
- Statement of Applicability (inclusion with rationale /exclusion with justification)

Based on the RA report, Information System Security teams prepare the RTP, which includes selection of controls. The accel bi then obtains management approval for RTP implementation and acceptance of residual risk.

Ref: ORM600 Risk Management (Project)

Ref: ORS600 Asset Management

Ref: ORS610 Risk Assessment Sheet, QMO210 Information Security Risk Log

6.2 Information security objectives and planning to achieve them

accel bi Shall establish information security objectives at relevant functions and levels. The objectives shall:

- be consistent with the information security policy;
- be measurable (if practicable);
- take into account applicable information security requirements, and results from risk assessment and risk treatment;
- be communicated; and
- Be updated as appropriate.
- accel bi shall retain documented information on the information security objectives.

Following are the IMS Objectives established by senior management:

IMS Objectives:

a) Maintain confidentiality and integrity of the information

b) Availability of information to authorized users when needed

c) Meet regulatory and legislative requirements

d) Produce, maintain and test Business Continuity plans as far as practicable

e) Train all staff on information security

f) Report and investigate all breaches of information security and suspected weaknesses

g) Monitor Risk Treatment Plan and measure effectiveness of selected controls.

When planning how to achieve its information security objectives, accel bi monitor it's Quality & IMS Objectives.

Refer: Quality Objective Data Sheet "ORO500 Objective Monitoring Data"

Monitoring and analysis is carried our as follows:

a) Monitoring and measurement of the controls shall be done as per process mentioned in the template.

b) System Administrator either himself or shall make one of the data center employee responsible for monitor and measurement of controls.

c) The results from monitoring and measurement shall be analyzed and evaluated at least on monthly basis. However this analysis can be made early depending on the exigencies and system administrator shall decide the same.; and

d) System Administrator shall analyze and evaluates these results.

Refer: IMS Objective Monitoring sheet: ORO500 Objective Monitoring Data

7 Support

7.1 Resources

The management provides resources for the implementation, maintenance, and review of the ISMS. The resources include funds, tools, human resources and any other resources that may be required for the efficient performance of the ISMS.

Periodically the accel bi evaluates resource requirements for improvements in security infrastructure based on RA, review /audit records. Based on resource requirements, the Management approves/ allocates the required resources.

7.2 Competence

Personnel who have experience and expertise in the application domain and in information security concepts are assigned to manage ISMS. Whenever feasible, experienced individuals are available and allocated appropriate responsibilities. When the required levels of skill and expertise are not available, trainings are provided to ensure skill / knowledge enhancement as per the accel bi training process.

The IMS training should form an integral part of training curriculum of HR Dept. in association with IMS Team.

- Identifying what training is needed, and how frequently, for specific positions.
- Identifying qualified individuals/agency to conduct the training program.
- Organizing the training program.
- Maintaining attendance records, course outlines and course feedback of all trainings conducted.

The accel bi maintains records of all training programs as mentioned in the training process.

Ref: Procedure for Training: ORM570 Talent Development Process,

Ref: ORS910 Productivity Management Process

Ref: ORS920 Rewards Management Process

Ref: ORS940 Talent Empowerment Process

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- the information security policy;
- their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- The implications of not conforming to the information security management system requirements.
- All updates in organization policies & procedure, which are relevant to their job function

Ref: ORS940 Talent Empowerment process

7.4 Communication

Users shall be made aware about the risk of Information Security while exchanging information through Voice, Email, Fax, and Video Communication facility.

Ref: ORM400 Communication Management

7.5 Documented information

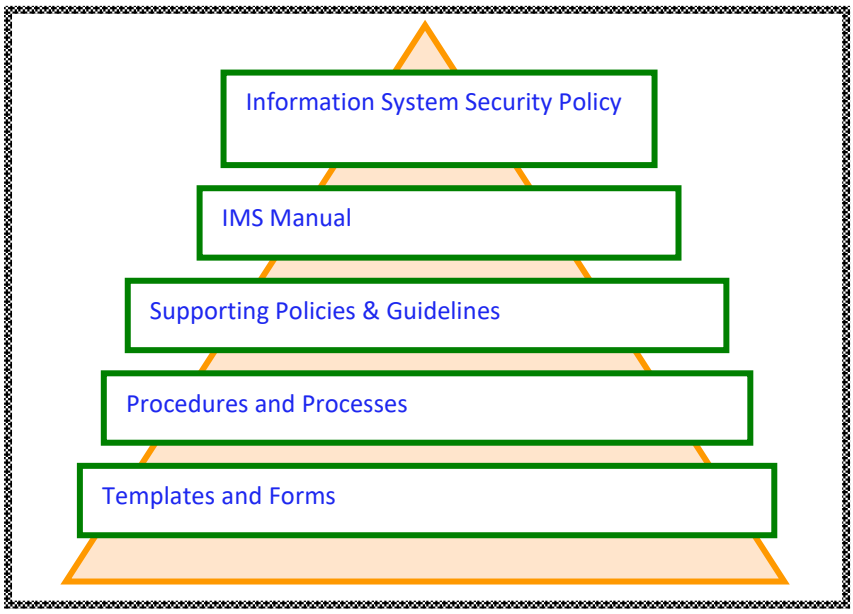
7.5.1 General

The organization's information security management system shall include:

a) Documented information required by this International Standard; and

b) Documented information determined by the organization as being necessary for the effectiveness of the information security management system.

To meet the requirement of 7.5, the documentation structure of Information security management System is as detailed below:



The components of IMS Documentation are:

Level - 0 Information System Security Policy: It is the Top-level security policy of the accel bi

Level - 1 Manual - This document includes requirements of the ISO/IEC 27001:2013 standard, and describes how the defined IMS meet the requirements. The document details the accel bi approach towards management and implementation of ISMS.

Level - 2 Supporting Policies & Guidelines - A complete set of supporting IMS policies and guidelines as identified and defined by the accel bi within the scope of ISMS.

Level - 3 Procedures and Processes – Contains processes and procedures required for implementing and supporting the defined policies & guidelines.

Level - 4 Templates and Forms – accel bi standard templates/forms used in the processes / procedures. These are used to streamline the operation of IMS and form a basis for records.

7.6 Creating and updating

When creating and updating documented information the accel Bi shall ensure appropriate:

A. Identification and description (e.g. a title, date, author, or reference number);

B. Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

C. Review and approval for suitability and adequacy.

7.6.1 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, accel bi address the following activities, as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including the preservation of legibility;

c) control of changes (e.g. version control); and

d) Retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the Quality & information security management system, shall be identified as appropriate, and controlled.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

7.7 Control of Documents

All documents related to IMS requirements are controlled as per 'accel bi- -DRM-Document & Record Management Procedure'

This includes:

- Review and approval of documents for adequacy prior to issue / use
- Updating, review and approval of necessary changes in controlled documents
- Availability of current revisions of necessary documents
- Withdrawal of obsolete documents from all points of issue or use to ensure guarding against unintended use.
- All security documents are available on the Intranet for reference and use based on need-to-know requirements.
- Any document if printed is considered obsolete. However, this excludes all the documents related to 'Business Continuity Plan QMPLAN10'

7.8 Control of Records

Records are identified within each procedure in the IMS to provide evidence of conformance to requirements and effective functioning of the ISMS. Master list of records is maintained. Other attributes shall be as per 'accel bi' Information Classification, Labeling and Handling Policy.docx'

- Ref: QMS100 Document & Record Management Procedure
- Ref: QMO110 Master List of Documents
- Ref: QMO120 Master List of Records
- Ref: QMO120 Master List of External Documents

8 Operation

8.1 Operational planning and control

8.1.1 Implement and Operate the ISMS

Selected control objectives, and controls that are a part of RTP are implemented effectively in accel bi and they are also capable of enabling prompt detection of and response to security incidents.

accel bi ensures that proper training and awareness on IMS are conducted, and appropriate resources are assigned to manage IMS.

accel bi control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

accel bi ensure that outsourced processes are determined and controlled

accel bi maintains a suitable matrix of risk / incidence reduction against its major controls identified every year for monitoring purposes to ensure effectiveness of selected controls. Logs of risk reduction and/or incidence reduction are maintained for results comparison and reproduction.

Ref: ORM200 Project management

8.2 Requirements for products and services

8.2.1 Customer communication

Communication with customers include:

A. Providing information relating to products and services;

B. Handling enquiries, contracts or orders, including changes;

C. Obtaining customer feedback relating to products and services, including customer complaints;

D. Handling or controlling customer property;

E. Establishing specific requirements for contingency actions, when relevant.

Ref: ORM400 Communication Management

8.2.2 Determining the requirements for products and services

When determining the requirements for the products and services to be offered to customers, the accel bi ensure that:

A. the requirements for the products and services are defined, including:

   1. any applicable statutory and regulatory requirements;

   2. those considered necessary by the organization;

B. the organization can meet the claims for the products and services it offers.

8.2.3 Review of the requirements for products and services

accel bi ensure that it has the ability to meet the requirements for products and services to be offered to customers. accel bi conduct a review before committing to supply products and services to a customer, to include:

a) Requirements specified by the customer, including the requirements for delivery and post delivery activities;

b) Requirements not stated by the customer, but necessary for the specified or intended use, when known;

c) Requirements specified by the organization;

d) Statutory and regulatory requirements applicable to the products and services;

e) Contract or order requirements differing from those previously expressed.

accel bi ensure that contract or order requirements differing from those previously defined are resolved. The customer's requirements are confirmed by the organization before acceptance, when the customer does not provide a documented statement of their requirements. NOTE In some situations, such as internet sales, a formal review is impractical for each order. Instead, the review can cover relevant product information, such as catalogues.

The accel bi retain documented information, as applicable:

a) on the results of the review;

b) on any new requirements for the products and services.

Ref: BDM100 Capture Process

Ref: BDM200 Proposal Process

Ref: BDM500 Process for Contract Acceptance

Ref: BDM920 Transition to operations team

8.2.4 Information security risk assessment

accel bi shall perform Quality & information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in Risk assessment process. accel bi retains documented information of the results of the information security risk assessments & relevant changes.

Ref: Risk Assessment sheet QMO210 Information Security Risk Log

8.2.5 Information security risk treatment

accel bi shall implement the information security risk treatment plan.

accel bi retains documented information of the results of the information security risk treatment.

Ref: QMS200 Risk treatment plan

Ref: QSPLAN10 Business Continuity procedure

8.3 Design and development of products and services

Requirements of clause 8.3 Product Design & Development are not applicable to accel bi as, we are providing services to customer as per customer specifications & guidelines mentioned in contract agreements

8.4 Control of externally provided processes, products and services

accel bi ensure that externally provided processes, products and services conform to requirements. accel bi determine the controls to be applied to externally provided processes, products and services when:

1. products and services from external providers are intended for incorporation into the organization's own products and services;
2. products and services are provided directly to the customer(s) by external providers on behalf of the organization;
3. a process, or part of a process, is provided by an external provider as a result of a decision by the organization.

accel bi determine and apply criteria for the evaluation, selection, monitoring of performance, and re-evaluation of external providers, based on their ability to provide processes or products and services in accordance with requirements.

accel bi retain documented information of these activities and any necessary actions arising from the evaluations.

Ref: BDM400 Process for Procurement Process

8.4.1 Information for external providers

accel bi ensure the adequacy of requirements prior to their communication to the external provider. accel bi communicate to external providers its requirements for:

a) the processes, products and services to be provided;

b) the approval of:

1) products and services;

2) methods, processes and equipment;

3) the release of products and services;

c) competence, including any required qualification of persons;

d) the external providers' interactions with the organization;

e) control and monitoring of the external providers' performance to be applied by the organization;

f) verification or validation activities that the organization, or its customer, intends to perform at the external providers' premises.

Ref: BDM400 Process for Procurement Process

8.5 Production and service provision

8.5.1 Control of production and service provision

accel bi implement production and service provision under controlled conditions. Controlled conditions shall include, as applicable:

a) the availability of documented information that defines:

1) the characteristics of the products to be produced, the services to be provided, or the activities to be performed;

2) the results to be achieved;

b) the availability and use of suitable monitoring and measuring resources;

c) the implementation of monitoring and measurement activities at appropriate stages to verify that

1. criteria for control of processes or outputs, and acceptance criteria for products and services, have been met;

d) the use of suitable infrastructure and environment for the operation of processes;

e) the appointment of competent persons, including any required qualification;

f) the validation, and periodic revalidation, of the ability to achieve planned results of the processes

1. for production and service provision, where the resulting output cannot be verified by subsequent monitoring or measurement;

g) the implementation of actions to prevent human error;

h) the implementation of release, delivery and post-delivery activities.

Ref: ORM200 Project Management

Ref: BDM800 Talent Acquisition process

Ref: ORS550 On Boarding Process

Ref: BDM700 Delivery Process

8.5.2 Identification and traceability

accel bi use suitable means to identify outputs when it is necessary to ensure the conformity of products and services.

accel bi identify the status of outputs with respect to monitoring and measurement requirements throughout production and service provision.

accel bi control the unique identification of the outputs when traceability is a requirement, and shall retain the documented information necessary to enable traceability.

Ref: QMS100 Document & Record Management Procedure

Ref: BDM700 Delivery Process

8.5.3 Property belonging to customers or external providers

accel bi exercise care with property belonging to customers or external providers while it is under the organization's control or being used by the organization.

accel bi identify, verify, protect and safeguard customers' or external providers' property provided for use or incorporation into the products and services.

When the property of a customer or external provider is lost, damaged or otherwise found to be unsuitable for use, accel bi report this to the customer or external provider and retain documented information on what has occurred.

Ref: BDM700 Delivery Process

Ref: ORS990 Separation Process

Ref: ORM700 Project Closure

8.5.4 Preservation

accel bi preserve the outputs during production and service provision, to the extent necessary to ensure conformity to requirements.

NOTE Preservation can include identification, handling, contamination control, packaging, storage, transmission or transportation, and protection.

8.5.5 Post-delivery activities

accel bi meet requirements for post-delivery activities associated with the products and services. In determining the extent of post-delivery activities that are required, accel bi consider:

a) statutory and regulatory requirements;

b) the potential undesired consequences associated with its products and services;

c) the nature, use and intended lifetime of its products and services;

d) customer requirements;

e) customer feedback.

NOTE Post-delivery activities can include actions under warranty provisions, contractual obligations such as maintenance services, and supplementary services such as recycling or final disposal.

8.5.6 Control of changes

accel bi review and control changes for production or service provision, to the extent necessary to ensure continuing conformity with requirements.

accel bi retain documented information describing the results of the review of changes, the person(s) authorizing the change, and any necessary actions arising from the review.

Ref: ORM200 Project Management

8.6 Release of products and services

accel bi implement planned arrangements, at appropriate stages, to verify that the product and service requirements have been met.

The release of products and services to the customer shall not proceed until the planned arrangements have been satisfactorily completed, unless otherwise approved by a relevant authority and, as applicable, by the customer. accel bi retain documented information on the release of products and services. The documented information include:

a) evidence of conformity with the acceptance criteria;

b) traceability to the person(s) authorizing the release.

Ref: BDM700 Delivery Process

8.7 Control of nonconforming outputs

accel bi ensure that outputs that do not conform to their requirements are identified and controlled to prevent their unintended use or delivery. accel bi take appropriate action based on the nature of the nonconformity and its effect on the conformity of products and services. This shall also apply to nonconforming products and services detected after delivery of products, during or after the provision of services. accel bi deal with nonconforming outputs in one or more of the following ways:

A. correction;

B. segregation, containment, return or suspension of provision of products and services;

C. informing the customer;

D. obtaining authorization for acceptance under concession.

Conformity to the requirements shall be verified when nonconforming outputs are corrected.

accel bi retain documented information that:

A. describes the nonconformity;

B. describes the actions taken;

C. describes any concessions obtained;

D. identifies the authority deciding the action in respect of the nonconformity

Ref: QMS400 Procedure for Incident handling & Corrective Actions

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

accel bi shall evaluate the Quality & information security performance and the effectiveness of the Quality & information security management system. accel bi shall determine:

a) what needs to be monitored and measured, including Quality & information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) The details of what needs to be measured are given in monitoring & measurement plan. NOTE: The methods selected should produce comparable and reproducible results to be considered valid.

d) Monitoring and measurement of the controls shall be done on daily basis.

e) System Administrator either himself or shall make one of the IT Services employee responsible for monitor and measurement of controls.

f) The results from monitoring and measurement shall be analyzed and evaluated at least on monthly basis. However this analysis can be made early depending on the exigencies and system administrator shall decide the same.; and

g) System Administrator shall analyze and evaluate these results.

h) accel bi retains appropriate documented information as evidence of the monitoring and measurement results.

Ref: ORM300 Performance Management

Ref: ORS940 Talent empowerment process

Ref: ORS920 Rewards Management process

9.2 Monitor and Review the ISMS

accel bi ensures that IMS is properly monitored and reviewed periodically.

a) For monitoring incidents, the accel bi has a well-defined Incident Management Procedure, which ensures that all problems, errors identified during processing of any information are handled promptly and effectively, and breach of security is appropriately addressed. Refer QMS400 Incident Management Process'.

b) A process for conducting Management Reviews and audit procedure of IMS exists. The focus of the review is to ensure that IMS is effective, and all policies, controls and security objectives are in line with business requirements. The audit focuses on the compliance of accel bi's practices as defined in ISMS. Refer ' IMS Plan Process of Internal Audit QMS300'

c) Information Management System Committee reviews the level of residual and acceptable risks based on the changes in the deployed technology, new threats and vulnerabilities and business objectives. Refer 'QMS200 Risk Assessment & Risk Treatment Procedure'

d) The controls at appropriate intervals are monitored against the logs generated to arrive at the current risk exposure. This is compared with previous risk level to verify the effectiveness of controls. Refer 'ORS200 CEM-Control Effectiveness Measurement Process'

9.3 Maintain and Improve the ISMS

Based on the review reports and audit findings, appropriate corrective and preventive actions, as approved by the Information System Security Committee are implemented and incorporated into the ISMS. Inputs for improvement can be from:

- Audit Reports

- Management Review Reports
- Incident Reports
- RA report
- Business Changes (Objectives, process, industry practices, legal/regulatory, etc.)
- Environmental Change (New threats and vulnerabilities, technology Changes, etc.)

accel bi maintains all inputs in an improvement database available for internal use, consolidates the inputs, and reviews the IMS for applicable improvements. For changes to be made, accel bi prepares an action plan and communicates the results to all interested /affected parties. All improvements should be directed towards predefined organizational Business objectives.

9.4 Internal Audits

CISO/IMS Coordinator conducts internal IMS audits half yearly to verify the adherence to IMS. The audits are conducted to ensure that IMS:

- Conforms to the requirements of the ISO/IEC 27001:2013 & ISO9001:2015 standard
- Ensure compliance with relevant legal, statutory and contractual requirements
- Conform to the identified Quality & information security requirements
- IMS is effectively implemented and maintained
- Performs as expected

Internal Audits are conducted in accordance with the audit procedure defined in 'QMS300 Internal Audit Procedure'**.** Trained personnel, not having direct responsibility of the activity being audited, shall conduct audits. CISO with the help of HODs will ensure that any non-conformance found is closed. CISO is responsible for planning, scheduling, organizing and maintaining records of these audits.

Ref: QMS300 Internal Audit Procedure

9.5 Management Review

Top management shall review Quality & information security management system once every six months, or on an event-driven basis, to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:

a) The status of actions from previous management reviews;

b) Changes in external and internal issues that are relevant to the Quality & information security management system;

c) Feedback on the Quality & information security performance, including trends in:

   1. nonconformities and corrective actions;
   2. monitoring and measurement results;
   3. audit results; and
   4. Fulfillment of Quality & information security objectives;

d) feedback from interested parties;

e) Results of risk assessment and status of risk treatment plan; and

f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the Quality & information security management system.

accel bi shall retain documented information as evidence of the results of management reviews.

Ref: ORS200 Management Review Procedure

9.6 Improvement

9.6.1 Nonconformity and Corrective Action

When nonconformity occurs, accel bi shall:

a) react to the nonconformity, and as applicable:
   1. take action to control and correct it; and
   2. deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1. reviewing the nonconformity;
   2. determining the causes of the nonconformity; and
   3. determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) Review the effectiveness of any corrective action taken; and

e) Make changes to the Quality & information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. accel bi retain documented information as evidence of:

a) The nature of the nonconformities and any subsequent actions taken, and

b) The results of any corrective action.

The procedure is created, for implementing and tracking the correcting action.

Ref: QMS400 Procedure for Incident handling & Corrective Actions

9.7 Continual Improvement

The accel bi is responsible for continual improvement of the IMS for suitability and effectiveness.

Inputs to continual improvement can be:

- Change in security policies and objectives
- Audit results and Management Review Reports
- Incident Reports
- Analysis of monitored events
- Corrective and Preventive Actions
- Business Changes
- Environmental Change (New threats and vulnerabilities)
- Best practices of industry

Ref: ORS920 Rewards Management Process

Ref: ORS910 Productivity Management Process ORS910

10 ISMS Controls

This section describes the selection and implementation of controls by accel bi. The control objectives and controls listed in this section are directly derived from the ISO/IEC 27001:2013 standard, based on **'Section 5.3.1 - Security Domains addressed in ISMS'** of this document.

Controls applicable to accel bi have been mentioned and addressed in this section. Controls not applicable to accel bi are not mentioned in this section and exclusion with justification given in SOA. Refer **'**QMSPLAN20 SOA**'**

A.5 Information Security policies

A.5.1 Management Direction for Information Security

Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Information Security Policy Document

Information System Security Policy document approved by the management exists. Information security policy documented in the **'IMS Manual** has been published and communicated to all employees of accel bi, through the Intranet and mails, training and induction programs.

A.5.1.2 Review of the policies for information security

accel bi is responsible for the creation, maintenance and updating of the policy. Information System Security Committee approves the policy prior to release. The review and evaluation of IMS policy is conducted at least once in a six months. The review guidelines state that the policy is to be reviewed against its effectiveness, compliance to business process, and compliance to technology changes. This is detailed in **section 9.3**.

A.6 Organization of Information Security

A.6.1 Internal organization

Control Objective: To manage information security within accel bi

A.6.1.1 – Information Security Roles and responsibilities

Security roles and responsibilities of employees, contractors and third party users are defined and documented in accordance with the organization's information security policy.

A.6.1.2 – Segregation of duties

In accel bi, duties have been segregated in order to reduce the risk of accidental or deliberate system misuse. Different individuals are responsible for their respective areas, and proper controls exist that take care of possibility of fraud in areas of single responsibility without being detected. Different areas and associated responsibilities are defined as per Roles and Responsibilities **Section 6.1.1**. Day to day administration & maintenance of IT Infrastructure is done by approved thirty party review different logs & conduct periodic verification carried out through internal audits.

A.6.1.3– Contact with authorities

Appropriate contacts/ agreements are maintained with the following but not limited to:

Services	Responsibility
Internet Service Provider (ISP)	VP Operations
Hardware Maintenance contracts	VP Operations
Telecom services department	VP Operations
Electricity services department	VP Operations
Local Enforcement Agencies like Police, Fire	VP Operations

Responsibility for any other services which fall under Information Security preview, but not mentioned above, is assigned to VP Operations. This is necessary to ensure that appropriate actions can be promptly taken, and advice obtained in the event of any security incident. Third party legal department is consulted for all third party contracts and agreements.

A.6.1.4 – Contact with special interest groups

Information security advice is obtained from vendors, legal advisors and technical experts on security matters to maximize the effectiveness of the ISMS. Internally CISO shall act as Security Advisor. External advice shall only be sought by CISO if required. All security incidents and breaches are reported to MR for necessary corrective and preventive actions.

A.6.1.5 – Information Security in Project Management

Project Planning, Monitoring and Control shall take care of information security in project management, which is defined in 'ORM200 Project Management Process'

A.6.2 Mobile Devices and Tele Working

Control Objective: To ensure information security when using mobile computing and tele working facilities.

A.6.2.1 – Mobile Device Policy

accel bi has well defined policy and guidelines on the use of laptops. Refer 'PLIT02 -Use of Mobile Device / Laptops Policy'.

A.6.2.2 – Tele working

accel bi has a well-defined policy and guideline on the use of laptops/mobile's for teleworking purposes. Refer 'PLIT02 Tele working Policy'

A.7 Human Resource Security

A.7.1 Prior to employment

Control objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

A.7.1.1 –Screening

accel bi has a documented recruitment process. 'BDM800 Talent Acquisition Process'. The screening requirements form part of contract agreement with vendors.

A.7.1.2 – Terms and conditions of employment

All employees of, accel bi, at the time of joining, are required to agree and sign the Terms and Conditions of employment as detailed in 'ORS550 - On Boarding Process'**.** The Terms and Conditions also state the employees' responsibility for Information Security.

A.7.2 During employment

Control Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

A.7.2.1 – Management responsibilities

Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

A.7.2.2 – Information security awareness, education and training

accel bi Ensures that users (employees and the relevant external parties) are made aware of their security responsibilities through ongoing awareness training programs. All employees are to adhere them while executing the Roles and Responsibilities as defined.

A documented procedure for training exists. accel bi, in association with HR Dept. ensures that all, accel bi personnel are imparted IMS related training and that a training module on Information security policies becomes an integral part of induction training programs. Refer 'ORS940 -Talent Empowerment Process'

A.7.2.3 – Disciplinary process

Any violation of the signed documents is considered as a disciplinary offence and as such act as a deterrent to employees who might otherwise be inclined to disregard security procedures. The procedure shall ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security. It is addressed by the reference to accel bi Conduct, Disciplinary and Appeal (CDA) Rules. Refer "PLHR05 Disciplinary Action Process".

A.7.3 Termination or change of employment

Control Objective: To ensure that employees, contractors and third parties exit, accel bi or change employment in an orderly manner.

A.7.3.1 – Termination or change of employment responsibilities

Responsibilities for performing employment termination or change of employment are clearly defined and assigned. Refer to accel bi Conduct, Disciplinary and Appeal (CDA) rules.

A.8 Asset Management

A.8.1 Responsibility for assets

Control Objective: To achieve and maintain appropriate protection of accel bi and its assets.

A.8.1.1 – Inventory of assets

accel bi's Assets have been classified as:

- **Hardware**– Includes computer equipment (CPU, Peripherals etc.), communication equipment (routers, switches, etc.), magnetic media (CDs, Tapes, Disks),UPS/Inverters / power backup devices/Battery Bank, Air conditioner ,Fire extinguisher etc.
- **Software** – Includes various applications programs, system software, development tools and utilities.
- **Information** –Databases, data files, archived information, documentation.
- **Services** – Include communication services, general utilities like power, AC, Buildings , Services (provided by org external/internal the group) etc.
- Management System- Includes Borrowed Information, Copyright/IPR, The whole Organization
- Human Resource- That include Technical Manpower & Administrative manpower

An inventory of all assets is maintained by the operations in the form of **Asset Register** accel bi maintains appropriate protection of the organizational assets. It aims at confidentiality, integrity, and availability.

Ref: ORO610 Infrastructure Asset Master List

Ref: ORO620 Software License List

Ref: ORO630 Data Asset List

A.8.1.2 – Ownership of assets

All information and assets associated with information processing facilities shall be owned by a designated part of the organization. The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.

A.8.1.3 – Acceptable use of assets

Rules for the acceptable use of information and assets associated with information processing facilities are identified, documented, and implemented. Ref to - EMHB01 Acceptable Use of Assets Guidelines in Employee Code of Conduct in Employee Handbook.

A.8.1.4 – Return of assets

All employees, contractors and third party users are required to return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

A.8.2 Information Classification

Control Objective: To ensure that information receives an appropriate level of protection.

A.8.2.1 – Classification of information

There are four levels of information classification defined in accel bi Refer 'PLIT12 Information Classification, Labeling and Handling Policy'

A.8.2.2 –Labeling of information

The guidelines for labeling and handling of Information in accel bi are documented and available in 'PLIT2 Information Classification, Labeling and Handling Policy'

A.8.2.3 –Handling of assets

accel bi has well defined guidelines for information labeling, handling and storage in order to protect information from unauthorized disclosure or misuse. Refer 'PLIT12 Information Classification, Labeling and Handling Policy

A.8.2.4 – Return of assets

All employees, contractors and third party users are required to return all of the organization's assets in their possession upon termination of their employment, contract or agreement. Refer 'ORS990 - Separation Process'.

A.8.3 Media handling

Control Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruptions to business activities.

A.8.3.1 – Management of removable media

All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications. accel bi has defined procedure for the management of computer media containing sensitive data. Refer – PLIT05 Media Handling Process'.

A.8.3.2 – Disposal of media

accel bi has defined procedure for the disposal of computer media. The Tapes, CDs and Hard Disks have been covered in 'PLIT05 - Removable Media Policy'.

A.8.3.3 – Physical media transfer

Backup media, Floppy, CD, Hardcopy etc. being transported from one location to the other is protected from unauthorized access, misuse and corruption by sending them through trusted, accel bi employee with proper authorization and adequate protection. Refer 'PLIT12 - Information Classification, Labeling and Handling Policy'.

A.9 Logical Security /Access Control

A.9.1 Business requirement for access control

Control Objective: To restrict access to information and information processing facilities.

A.9.1.1 – Access control policy

accel bi has implemented access control to information based on the business requirements and security requirements on 'need-to-know' basis. Well-documented access control policy and procedures are in place. Refer 'PLIT10 IT Access control Policy'

A.9.1.2 – Access to network and network services

The access to internal and external network of accel bi is controlled. This includes any direct access to services that are business critical to users within the domain, and direct access to network from users in high-risk location like users through Internet. Users shall only have direct access to the services that they have been specifically authorized to use. A defined and documented policy for use of network services exists. Refer PLIT10 - Internet Usage Policy'.

A.9.2 User access management

Control Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

A.9.2.1 – User registration& deregistration

accel bi has well defined policy and procedure for managing user access to all information systems and services. Refer 'PLIT10 -IT Access control Policy'

A.9.2.2 – User access provisioning

A unique login id and password has been assigned to all users, with varying privileges, depending on roles, and requirements. User identification and authentication is implemented in accordance with privileges granted to the respective user. Refer 'PLIT10 - IT Access control Policy'

A.9.2.3 – Management of Privileged Access rights (Password Policy)

The allocation and use of privileges is restricted and controlled. Any privilege given onto any system in accel bi is covered. Refer 'PLIT10-IT Access control Policy'

A.9.2.4 – Management of Secrete Authentication information of users (Password Management)

accel bi has a well-defined password policy and guidelines. Refer 'PLIT10 - IT Access control Policy'.

A.9.2.5 – Review of user access rights

User privileges for accel bi will be reviewed every three months and for global users it will be reviewed once every year. System Administrator shall review the access rights & respective Business Owner shall ratify the review report.

A.9.2.6 – Removal or adjustment of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.3 User Responsibilities

Control Objective: To prevent unauthorized user access, and compromise on theft of information and information processing facilities.

A.9.3.1 – Use of Secret Authentication Information

accel bi has a well-defined password usage guideline for users to follow. Refer 'PLIT01 -Password Policy'.

A.9.4 Operating system access control

Control Objective: To prevent unauthorized access to systems and applications.

A.9.4.1– Information access restriction

Unauthorized access to information is restricted. Refer **'**PLHR02 - Employee Internet Use Monitoring and Filtering Policy'.

A.9.4.2 – Secure log-on procedures

All user machines are accessible through a user name and password. These are assigned to each authorized user and are unique in nature. Unauthorized access is not permitted. Refer **'**PLIT10 - Access control Policy' and 'PLIT08 - Virtual Private Network (VPN) Policy'

A.9.4.3 – Password management system

accel bi has a well-defined password policy and access management process. Refer 'PLIT01 - Password Policy & PLIT10 - IT Access control Policy'.

A.9.4.4 – Use of system utilities (Privileged utility programs)

All system utility programs, which impact the operations of the systems, are accel bi allowed with controlled access to administrative accounts. System Utilities are controlled.

A.9.4.5 – Access control to program source code

Source code and program libraries are not accessed by unauthorized people. Code management of IT related applications is being performed according to **'QMS100** - Control of Documented Information'

A.10 Cryptography

A.10.1 Cryptographic Controls

Control Objective: To protect the confidentiality, authenticity, or integrity of information by cryptographic means.

A.10.1.1 – Policy on the use of cryptographic controls

Refer 'PLIT11- Policy on the use of cryptographic controls

A.10.1.2 – Key Management

Refer 'PLIT11 - Policy on the use of cryptographic controls'

A.11 Physical and environmental security

A.11.1 Secure areas

Control objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

A.11.1.1 – Physical security perimeter

accel bi has a well-defined policy on physical security and procedure on physical access control. accel bi has implemented different security barriers to check the access into the premises.

- accel bi has main entry and exit point manned by security personnel.
- Entry to company premises for the employees is through biometric /access card and for visitors is through visitors pass.
- Access to specific /secure areas like server rooms is monitored through access card.
- Video Surveillance will be done through cameras accel bi allowed at critical location.

A.11.1.2 – Physical entry controls

Secured areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.1.3 – Securing offices, rooms, and facilities

accel bi has taken the following security measures:

- All employees, visitors and contract staff is supposed to report for security check-in and check-out formalities
- Entry is restricted to authorize personnel
- Each workstation, cubicle and cabin is provided with storage space, with lock and key arrangement to keep official documents/company classified information belonging to the employee of the workspace.
- Employees working after office hours enter their names, and sign –in and sign-out in a separate register maintained by the security guard on duty.

A.11.1.4 – Protecting against external and environmental threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster are designed and applied.

A.11.1.5 – Working in secure areas

Physical protection and guidelines for working in secure areas are:

- Unsupervised work within server room will be strictly prohibited for safety reasons.
- Personnel shall only be aware of the existence of, or activities within, a secure area on a need to know basis
- Eating and consuming other food products will be strictly prohibited in secure areas.
- Photographic, video, audio or other recording equipment should not be allowed, unless authorized permission.

A.11.1.6 – Delivery and loading areas

The delivery and handling of material is strictly under the authorization control with material gate pass. Without proper gate pass, no material is allowed to enter or leave the premises.

A.11.2 Equipment

Control Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

A.11.2.1 – Equipment sitting and protection

All equipment's are physically protected from security threats and environmental hazards, by positioning them at secure areas. Only authorized personnel can enter secured areas. The controls are adopted to minimize the risk of potential security threats. The following practices are being followed in accel bi,

- Business critical equipment are installed in server room, which is fully secured under lock and key
- Fire and smoke alarms are deployed appropriately.
- The information processing and storage facilities are fully secured
- Users are not allowed to have drink, eatables & smoke in the server room.
- Temperature and humidity levels are continuously monitored and maintained.
- Power equipment is periodically serviced and checked.

The procedure for maintaining proper temperature and humidity is provided as per 'PLIT01 – BYOD Policy.

A.11.2.2 – Supporting utilities

All IT equipment's are protected from power failure and other electrical anomalies. Arrangements are made to provide uninterrupted power supply (UPS) to all critical information processing facilities. UPS are maintained as per the OEM's instructions and covered under AMC contract. Lighting protection is provided to the building, which are turned on in case of failure or routine power cuts.

A.11.2.3 – Cabling security

The power and data cables are well protected and isolated in order to protect from interception and damage. All the cables (data, telecommunication, and electrical) are laid using proper conduits, in order to protect them from external damage. Power cables and network cables are well separated to prevent any interference.

A.11.2.4 – Equipment maintenance

All equipment's in accel bi PMO Office are being correctly maintained to ensure their continued availability and integrity. Adhering to the following steps ensures this:

- All equipment's are maintained in accordance with the OEM's recommendations for service intervals and specifications.
- All critical equipment's are covered under Service plan with the vendor.
- All equipment's are under the regular preventive maintenance.

A.11.2.5 – Removal of assets

All the equipment's that are taken out of the accel bi follow a proper authorization process. A proper gate pass is to be signed by the IT Manager before taking any equipment out of the accel bi.

A.11.2.6 – Security of equipment and assets off- premises

The person carrying the equipment outside the premises is responsible for the security of the equipment. accel bi has a documented policy for Laptops and portable media taken outside premises. Refer 'ORS600 - -Asset Management'.

A.11.2.7 – Secure disposal or re-use of equipment

The information available on equipment's is removed or erased before the equipment disposal. The information available on equipment's, which is re-used for some other purposes, is removed or erased before the equipment is re-used. The information available on media, which is re-used for some other purposes, is removed or erased

before the media is re-used. All defective computer media, to be disposed, is destroyed completely and all relevant information is made irrecoverable. Refer 'ORS600 - -Asset Management'.

A.11.2.8 – Unattended user equipment

A well-defined policy exists at accel bi regarding equipment's unattended for a long duration. Refer'. PLIT17 - IT Access control Policy'

A.11.2.9 – Clear Desk and Clear screen policy

Personal computers are not left logged on when not in use and are protected by password. The screen saver is password protected. Refer 'PLHR07 - Clear Desk & Clear Screen Policy'.

A.12 Operations Security

A.12.1 Operational procedures and responsibilities

Control Objective: To ensure the correct and secure operation of information processing facilities.

A.12.1.1 – Documented operating procedures

accel bi has a set of defined operating manuals for processing the department functionality. All documented operating manuals are identified in the 'ORS600 Assets Management'.

A.12.1.2 –Change management

Whenever a change in the IT infrastructure is to be done, a proper evaluation and analysis is done which includes cost, security, technical functionality and compatibility. Any user can initiate change request. Manager/IT is authorized to initiate the change & Head/IT approves these operational and process changes. To control all operational changes accel bi has defined policy. Refer 'PLDB01 - Change Management Policy'

A.12.1.3 – Capacity management

It is the responsibility of the individual managers to look for capacity demands for their projects in advance. This ensures that the required capacity can be arranged in time to minimize the risk of failure due to lack of capacity. It also ensures the continuous availability of operational systems. Utilization of existing resources is monitored regularly. Refer 'ORM200 Project Management'.

A.12.1.4 – Separation of development, test and operational facilities

The development and testing activities shall not be done in production environments. These environments are separately maintained in Cloud environments.

A.12.2 Protection from Malware

Control Objective: To protect the integrity of software and information processing facilities are protected against malware.

A.12.2.1 – Controls against malicious code

Precautions are required to prevent and detect the introduction of malicious software. Software information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses, and logic bombs etc. accel bi has implemented several controls to address the threat:

- accel bi has a policy for prevention against malicious software.
- accel bi has a policy for the use of networks or any other medium as a preventive measure against virus attacks.
- Virus attacks and software malfunctions due to malicious software are treated as security incidents and handled.
- To prevent loss of data due to malicious software regular backups of critical data are taken regularly.

Refer 'PLIT17 Server Malware Protection and Antivirus Policy'

A.12.3 Back-up

Control Objective: To maintain the integrity and availability of information and information processing facilities.

A.12.3.1 – Information back up

Backup of informational Servers are taken regularly. accel bi has a well-defined procedure for Information backup and restoration. Refer 'PLIT14- Backup Policy'.

A.12.4 Logging and Monitoring

Control Objective: To detect unauthorized information processing activities

A.12.4.1 – Event logging

accel bi has defined policy for event logs. All systems are monitored to detect deviation from access control policy. This audit trail serves as evidence in case of security breach, and is the basis for any action. Audit logs are maintained on servers and provide audit information related to User Id, Date and time of log-on and log-off, failed login attempts, Terminal Location. Refer 'PLIT08 - Virtual Private Network (VPN) Policy'.

A.12.4.2 – Protection of log information

Logging facilities and log information are protected against tampering and unauthorized access.

A.12.4.3 – Administrator and operator logs

Logging facilities and log information are protected against tampering and unauthorized access.

A.12.4.4 – Clock synchronization

The correct setting of critical computer clocks is important and carried out to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases. One Server is identified as Time Master Server & other Servers of the network are synchronized with the Master.

A.12.5 Control of operational software

Control Objective: To ensure the integrity of operational systems.

A.12.5.1 – Installation of software on operational systems

To ensure secured implementation of Software on Operational System. Refer 'PLHR01 – working in Secured Area and PLIT07 – Access Control Policy'.

A.12.6 Technical Vulnerability Management

Control objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

A.12.6.1 – Management of technical vulnerabilities

accel bi is using VA/PT to obtain information on new exposures while applying patches for earlier identified threats and vulnerabilities. The VA/PT shall be carried out as per Security Committee Review Procedure. Appropriate actions will be initiated based on threat assessment diagnosed from VA/PT.

A.12.6.2 – Restrictions on software installation

Users should not run any unauthorized or undocumented software on their desktops. IT department will approve on the recommendation of Department Heads, the installation of any software on Desktop/Laptop/Servers. Refer 'ORS600 Asset Management' in section 7. Guidelines for Desktop/Laptop/Server users

A.12.7 Information systems audit considerations

Control Objective : To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

A.12.7.1- Information systems audit controls

Audit activities involving checks on operational system shall be carefully planned and agreed to minimize the risk of disruption to business processes.

A.13 Communications and Operations Management

A.13.1 Network security management

Control Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.13.1.1 – Network controls

accel bi has a dedicated team of employed professionals in network, who are responsible for the smooth and secure operation of the network. Policies of network usage are defined. Refer 'PLHR03 IEM-Internet & Electronic Messaging Usage Policy'.

A.13.1.2 – Security of network services

Security attributes for network services like Leased Line / Wireless Radio modem is taken care through SLA (Service Level Agreement) with ISP (Internet Service Provider) viz., STPI.

A.13.1.3 – Segregation in networks

Network is segregated as per policy defined in 'PLIT08 - Network Security Management Policy'.

A.13.2 Exchange of Information

Control Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

A.13.2.1 – Information transfer policies and procedures

The Electronic Office Systems like Telephone, Fax etc. are maintained by a 3rd Party. Security of Information available through such system is ensured through suitable clauses in the contract.

Users shall be made aware about the risk of Information Security while exchanging information through Voice, Fax, and Video Communication facility.

A.13.2.2 –Agreements on information transfer

Agreements shall be established for the exchange of information and software between accel bi and external parties like suppliers / contractors etc.

A.13.2.3– Electronic messaging

The electronic mail systems are properly secured from unauthorized access by using Spam protection software & Anti-Virus firewall, and from viruses by deploying antivirus software. accel bi has a well-defined policy and guidelines on the use of electronic mail. Refer 'PLHR03 -Internet & Electronic Messaging Usage Policy.

A.13.2.4 – Confidentiality or non-disclosure agreements

All contractors and external parties are required to sign NDA as covered by respective contract guidelines.

A.14 Systems acquisition, development and maintenance

A.14.1 Security requirements of information systems

Control Objective: To ensure that security is an integral part of information systems.

A.14.1.1 – Security requirements analysis and specification

accel bi, will acquire and accept hardware and software as per customer contract requirements. Refer 'BDM500 - Contract Acceptance', 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A.14.1.2 – Securing applications services on public networks

Accel bi, use secure VPN connection when accessing applications services on public network. Refer "PLIT07 - Virtual Private Network (VPN) Policy"

A.14.1.3 – Protecting application services transactions

Accel bi, use secure VPN connection when accessing applications services on public network. Refer "PLIT07 - Virtual Private Network (VPN) Policy"

A.14.2 Security in development and support processes

Control Objective: To maintain the security of application system software and information.

A.14.2.1 – Secure development policy

Software development will be as per the agreed Software Development Lifecycle described in 'BDM500 - Contract Acceptance'

A.14.2.2 – Change control procedures

accel bi follows change management process as per customer defined procedure to manage and control changes in the software developed and support systems, during the development life cycle. The process is negotiated during the contract acceptance and followed through project management and delivery management process. Refer 'BDM500 - Contract Acceptance', 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A.14.2.3 – Technical review of applications after operating system changes

The application systems are reviewed to ensure that there is no adverse impact on operation and security due to changes in operating system as per scope of work defined in contract acceptance process. Refer 'BDM500 - Contract Acceptance', 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A.14.2.4 – Restrictions on changes to software packages

Modification to software package is not permitted without the consent of project team. To ensure that only desired changes are implemented after the approval, a process need to be followed for controlling the changes in software packages. For this the process is defined 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A. 14.2.5 – Secure System Engineering Principles

Software development will be as per the agreed Software Development Lifecycle defined in 'BDM500 - Contract Acceptance'

A. 14.2.6 – Secure Development Environment

To secure the selected product of development environment the process of configuration management need to be adopted so that the correct product is available to authenticated users Refer 'PLHR07 - Procedures for working in secure areas' and 'PLIT10 - Access Control Policy'.

A.14.2.7 – Outsourced software development

accel bi does not outsource customer related software development activities. NOT APPLICABLE.

A. 14.2.8 – System security testing

System security testing process is defined in section 7.3 of 'BDM500 - Contract Acceptance'

A.14.2.9 – System acceptance testing

New information systems, upgrades, and new versions are put through a system acceptance for their acceptability and interoperability. A separate environment comprising of hardware and software is used to carry out tests prior to deploying or upgrading the main system. Appropriate tests are carried out to confirm that all acceptance criteria are fully satisfied. The tests results are documented and operational, maintenance and usage procedure are established. Training is provided for use and operation of new system. The process is negotiated during the contract acceptance and followed through project management and delivery management process. Refer 'BDM500 - Contract Acceptance', 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A.14.3 Test Data

Control Objective: To ensure the protection of data used for testing.

A.14.3.1 – Protection of test data

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data, hence test data is carefully selected and controlled such that security violations do not occur. The process is negotiated during the contract acceptance and followed through project management and delivery management process. Refer 'BDM500 - Contract Acceptance', 'ORM200 Project Management' and 'BDM700 Delivery Process'.

A.15 Supplier relationships

A.15.1 Security in supplier relationship

Control Objective: To maintain the security of accel bi's information and information processing facilities that are assessed, processed, communicated to, or managed by external parties or suppliers.

A.15.1.1 – Information security policy for supplier relationships

accel bi has identified risks from third-party access mainly in two categories viz., Physical and Network. Risk areas have been identified and appropriate measures shall be taken to mitigate them. They have been addressed adequately in the following sections of this chapter.

- A.11.1.2 – Physical entry controls
- A.9.1.2 – Access to network and network services

All contract personnel are given restricted access as per the requirement of the service they are providing and as per the contractual obligations. All third parties working at the premises have signed Non-Disclosure Agreement (NDA) at the time of contracts.

A.15.1.2 – Addressing security within supplier agreements

All agreements with the supplier who provides any type of services to accel bi & have access to the premises of accel bi shall have a clause related to security and Access Control as under

"The vendor will adhere to security guidelines of accel bi while delivering the services and follow access privileges & rights provided with precaution and safety measures indicated for each of them. Non-adherence of these guidelines may result in termination of the agreement and/ or claiming of liability/ damages caused due to non-adherence of these instruction."

A.15.1.3 – ICT (Information and Communication Technology) Supply chain

All agreements with the Information & Communication Technology service provider, who provides any such type of services to accel bi, shall have the requirements to address information security risk in the agreement.

A.15.2 Supplier service delivery management

Control Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 – Monitoring and review of supplier services

The services reports and records provided by the third party are regularly monitored and reviewed regularly.

A.15.2.2 – Managing changes to supplier services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Control Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 – Responsibilities and procedures

Incident management responsibilities and procedure exist to ensure a quick, effective, and orderly response to security incidents. Refer **'**QMS400-Incident Management Process**'**.

A.16.1.2 – Reporting information security events

Security events are defined as incidents that could cause unauthorized disclosure, modification, or destruction of, accel bi's information assets, or loss or destruction of the physical equipment associated with the computer systems, it's peripheral or network infrastructure components. Security incidents also include other aspects of security, such as carrying fire arms, or other lethal weapons on property, are as typically secured being left unlocked or unattended, fire or witnessing someone performing an unsafe act, or committing a violation of security policies or procedures etc. All users in the, accel bi are responsible to report any observed or suspected security incidents through email/help desk phone/on-line Incident reporting system available on Intranet. The security incidents are reported and are managed by the documented procedure. Refer **'**QMS400 - Incident Management Process**'**.

A.16.1.3 – Reporting information security weaknesses

Security weaknesses are defined as loopholes, weak points or vulnerabilities in the information system. These vulnerabilities or the loopholes may be exploited to gain unauthorized access to data or systems. All users in the, accel bi are responsible to note and report any such observed or suspected security weakness. Any user (viz., employee, contractor and third party) can report the incident using email/help desk phone/online system available on Intranet. They shall report these incidents as per **'**QMS400 - Incident Management Process**'**.

A.16.1.4 – Assessment and decision of information security events

All incidents occurring in the, accel bi are documented and stored and handled as per the procedure defined in QMS400 -Incident Management Process'

A.16.1.5 – Response to information security incidents

All incidents occurring in the, accel bi are documented and stored and handled as per the procedure defined in QMS400 - Incident Management Process

A.16.1.6 – Learning from information security incidents

All incidents occurring in the, accel bi are documented and stored in the Corrective and Preventive Actions database. The accel bi consolidates the incident reports for root cause analysis and considers these as an input for appropriate actions and necessary controls to avoid reoccurrence of the incidents.

A.16.1.7 – Collection of evidence

All applicable laws and regulations have been identified by, accel bi wherever applicable, the records and documents that may be accepted as evidence shall be collected and maintained. Shall ensure that all evidence collected in the process is:

- Admissible as evidence – Acceptable to court and legal authorities
- Complete – Present a complete trail of the incident
- Meet quality requirements – Are readable, legible etc.

A.17 Business continuity management

A.17.1 Information security aspects of business continuity management

Control objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure timely resumption.

A.17.1.1 – Planning information security continuity

Business continuity begins by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This is followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). This assessment considers all business processes and is not limited to the information processing facilities. Depending on the results of the risk assessment, a strategy plan is developed to determine the overall approach to business continuity. The details of BCP are detailed as per **'**QSPLAN10 BCP-Business Continuity Plan Process**'.**

A.17.1.2 – Implementing information security continuity

Implementing information security continuity shall covered in section 6.2.Identify critical resources & in section 7.2.Business Continuity Policies for the Organization in 'QSPLAN10-Business Continuity Plan Process'

A.17.1.3 – Verify, review and evaluate information security continuity

Business continuity plans shall be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plan(s) are detailed in the**'** QAPLAN10 - Business Continuity Plan Process**'.**

A.17.2 Redundancies

Control objective: To ensure availability of information processing facilities.

A.17.2.1 – Availability of information processing facilities

Information processing facilities shall be monitored and sufficient redundancy shall be ensured by fixing the appropriate threshold level while maintain Control Effectiveness Measurement as defined in the -Control Effectiveness Measurement Process

A.18 Compliance

A.18.1 Information security reviews

Control Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A.18.1.1 – Independent review of information security

Information System Security Committee is responsible for reviewing and auditing the IMS for its compliance. All areas covered in the IMS policy are considered for regular reviews and audits. CISO prepares and publishes the annual audit/ review plan. Details are mentioned in **Section 6** of this document.

A.18.1.2 – Compliance with security policies and standards

The , accel bi with the help of the Security Committee and other Core Group members conducts periodic/event-driven review to ensure compliance with security policy & standards.

A.18.1.3 – Technical compliance checking

Periodic internal audits, third party audits and independent VA/PT shall be planned for and conducted according to Security Committee Review Procedure.

A.18.2 Compliance with legal and contractual requirement

Control Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.

A.18.2.1 – Identification of applicable legislation

All relevant statutory, regulatory, and contractual obligations pertaining to information systems are explicitly defined and documented. accel bi adheres to all the applicable laws and acts. It is the responsibility of the HR department to review compliance and identify new or unidentified legal obligations. All agreements entered by the company are duly vetted and approved by the HR department for this purpose.

A.18.2.2 – Intellectual property rights (IPR)

accel bi ensures that all license agreements are respected and limits the use of the products to specified machines, and for specific purposes.

a) The IPR of hardware, software and documentation belonging to , accel bi will not be disclosed to any outside party unless and otherwise cleared by , accel bi

b) The IPR of programs and associated material supplied by outside organizations / collaborators will be used by, accel bi for only those purposes for which they are licensed.

c) No unauthorized copies will be made for use within or outside, accel bi

A.18.2.3 – Protection of documented information

The important records are protected from loss, destruction and falsification. The following records of, accel bi are safeguarded:

- Master List of Documents
- Master List of Records
- Database records
- Transaction logs
- All contracts and agreements

All records are retained for a defined period as specified by the owner of the information. Storage and handling of all these records is in accordance with a defined procedure. Refer ‘ORS930 -Compliance Process’

A.18.2.4 – Privacy and protection of personal information

Data protection Act is not applicable. However, all personal records are maintained as hard copies and classified as 'Confidential'. Only HR department has access to those files. Online personal information is maintained which is password protected, and the access is limited to the HR.

A.18.2.5 – Regulation of cryptographic controls

The cryptographic regulations as per IT Act 2008 of Government shall be followed for accel bi operations. In case of usage of third party cryptographic devices compliance letter from the third party shall be secured.

12. IMS Master list of Records and its Retention Period

Ref: QMO100 Master List of Documents

Ref: QMO110 Master List of Records

Ref: QMO120 Master List of External Documents