your logo here 

Audit Report

Initial Information Security Sample Assessment

 Watermark configurable in report template

Audit No 10
Audit / Assessment Lead Andy von Grebmer

Contents

Management Summary

Max. 10'000 Charaters. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Assessment Scope

Scope	Optional field. A short description of the scope of the audit e.g. HR Hiring Process, Product X Production process, The 2018 Global Change Project etc. Text, maximum of 3000 characters allowed.
Legal Entity	Finale Grande Ltd
Service	Service 3

All org. fields used shown here

Legal Entity	Melbourn Ltd
Site	P-CBlock
Department	PI-HR
Division	P-APAC
Business Function	P-Services
Business Process	P-Finance
Service	P-Professional

Conclusion

Needs Improvement

Assessor Recommendation(s)

Max. 10'000 Charaters. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Management Response

Max. 10'000 Charaters. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor

sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Control Domain Summary (Table)

Only filled if used

Control Domains	Total controls applicable	PASSED	PASSED WR	WORK IN PROGRESS	FAILED	N/A	Maturity Level	Implementation Status of applicable controls	Action items
BC - Business Continuity Management	8	1	1	5	1	0			6, 7
BM - Backup Management	7	0	1	5	1	0			8, 9
CF - Configuration Management	2	0	0	2	0	0			
CM - Change Management	3	0	0	3	0	0			
DPR - Data Protection Regulations	12	0	0	12	0	0			
IAM - Identity & Access Management	5	0	0	5	0	0			
IM - Information Security Management	17	0	0	17	0	0			
IN - Incident Management	4	0	0	4	0	0			
IO - Internal Organization	5	0	0	5	0	0			
OP - Operational Procedures	4	0	0	4	0	0			
PM - Project Management	8	0	0	8	0	0			
PS - Physical Security Management	3	0	0	3	0	0			
QM - Quality Management & Compliance	1	0	0	1	0	0			
RM - Risk Management	3	0	0	3	0	0			
SE - System Security Management	17	0	0	17	0	0			
SP - Service Provider Management	3	0	0	3	0	0			
Total score	102	1	2	97	2	0	N/A	0%	

Identified Issues and Corrective Actions

For the full details, please refer to section Control Evaluation Details.

Controls not directly passed, and related action item(s), if any

Grouping	Item	Status	Actions / Action items
BC - Business Continuity Management	BC02.0001 Procedures & Processes Business Continuity Strategy and Plan are available and up to date.	Failed	6 Action item to address a finding / impro...
BC - Business Continuity Management	BC02.0008 Procedures & Processes IT Business Continuity Plan is available and up to date.	Passed - Restrictions	7 Update role description for BCM.
BM - Backup Management	BM02.0001 Procedures & Processes Backup and restore procedures are in place.	Failed	8 Define backup retention policy.
BM - Backup Management	BM02.0002 Procedures & Processes Backup scope and requirements defined and business requirements applied.	Passed - Restrictions	9 Define RPO in all SLA and ensure monitor...

Reviewer Comments

Max. 1000 Charaters. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Introduction

Tenant Administrator: Please fill in this section in Report Template according to the organisational needs.

Audit Team

Lead	Andy von Grebmer	Signature____________________
Team Member	Heike Klaus	Signature____________________
Reviewer	Franz Mustermann	Signature____________________

Audit Dates

Start Date	2019-01-28
End Date	2019-02-08

Methodology

Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.

Methodology can be prefilled by changing the report template or user can change individually for each report in word.doc

Control Assessment Metrics

Status Label	Status description
Failed	Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.
Passed	Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.
Passed - Restrictions	Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.
Work in Progress	Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.

Review of the Documentation

Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.

Interviews

Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.

Data Analysis

Tenant Administrator: Please fill in this section in Report Template according to the organizational needs.

List of used Controls / Results

For the full details, please refer to section Control Evaluation Details.

Control Domain	Control ID	Control	Control Area	Result
Business Continuity Management	BC02.0001	Business Continuity Strategy and Plan are available and up to date.	Procedures & Processes	Failed
Business Continuity Management	BC02.0005	Geographical distance has to be considered for Disaster Recovery Sites (e.g. for hosted applications)	Procedures & Processes	Passed
Business Continuity Management	BC02.0008	IT Business Continuity Plan is available and up to date.	Procedures & Processes	Passed - Restrictions
Business Continuity Management	BC02.0009	Management reviews of the Business Continuity Plan and Organization.	Procedures & Processes	Work in Progress
Business Continuity Management	BC03.0004	Communication and training of IT Disaster Recovery Plan (DRP).	Organisation & Training	Work in Progress

Business Continuity Management	BC03.0005	Coordinator for IT Disaster Recovery is defined and in place.	Organisation & Training	Work in Progress
Business Continuity Management	BC03.0006	Actual version of IT Disaster Recovery Plan (DRP) is accessible by all people being part of the execution of the plan.	Organisation & Training	Work in Progress
Business Continuity Management	BC04.0001	Business Continuity Plan (BCP) has to be regularly tested.	Monitoring & Testing	Work in Progress
Backup Management	BM02.0001	Backup and restore procedures are in place.	Procedures & Processes	Failed
Backup Management	BM02.0002	Backup scope and requirements defined and business requirements applied.	Procedures & Processes	Passed - Restrictions
Backup Management	BM02.0003	Execution of backup procedure.	Procedures & Processes	Work in Progress
Backup Management	BM02.0004	Backup media inventory is required if backup media are handled manually (incl. transportation to another location).	Procedures & Processes	Work in Progress
Backup Management	BM02.0005	Storage and security of removable media is controlled.	Procedures & Processes	Work in Progress
Backup Management	BM02.0006	Storage of backups in an alternate location, detached from the primary location.	Procedures & Processes	Work in Progress
Backup Management	BM04.0001	Periodic restore tests are performed.	Monitoring & Testing	Work in Progress
Configuration Management	CF02.0001	An inventory of all IT Assets involved in processing information is managed.	Procedures & Processes	Work in Progress
Configuration Management	CF02.0004	Software License Management.	Procedures & Processes	Work in Progress
Change Management	CM02.0001	Change Management (CM) procedure(s) are available and up to date.	Procedures & Processes	Work in Progress
Change Management	CM02.0002	The Change Management Procedure(s) is linked to the respective Incident / Problem Management Procedure.	Procedures & Processes	Work in Progress

System Security Management	SE04.0005	Vulnerability Management.	Monitoring & Testing	Work in Progress
System Security Management	SE04.0006	Network Share Management.	Monitoring & Testing	Work in Progress
System Security Management	SE04.0007	Network connections are monitored and have adequate security settings.	Monitoring & Testing	Work in Progress
System Security Management	SE04.0013	Controlled Use of Administrative Privileges.	Monitoring & Testing	Work in Progress
System Security Management	SE04.0015	Email and Web Browser Protections.	Monitoring & Testing	Work in Progress
System Security Management	SE04.0016	Monitoring and reporting of limitations and Control of Network Ports, Protocols, and Services.	Monitoring & Testing	Work in Progress
System Security Management	SE05.0001	Malware protection is established and centrally managed.	Tools	Work in Progress
System Security Management	SE05.0004	Time synchronization management & time-synchronization technology.	Tools	Work in Progress
Service Provider Management	SP01.0002	Information Security & relevant compliance requirements are covered in vendor contracts.	Governance & Policy	Work in Progress
Service Provider Management	SP02.0001	Change Management of Vendor Services.	Procedures & Processes	Work in Progress
Service Provider Management	SP02.0003	Third party and supplier selection process.	Procedures & Processes	Work in Progress

Control Evaluation Details

All control details including mapped standards

Section with full details of each control in scope of the assessment.

Control Domain	Control	Control Area	Control ID	Status
Business Continuity Management	Business Continuity Strategy and Plan are available and up to date.	Procedures & Processes	BC02.0001	Failed

Control Requirements	Covered Standards
A Business Continuity Strategy and Plan is in place for all organizations and processes where the continued availability is required in case of a disaster or disruption. A defined level of resilience to incidents should be achieved. • Define a continuity strategy that meets the business requirements and ensure a resourceful implementation • Evaluate the relevant scenarios (threads) and their likelihood for the organization/process and the strategy how they are addressed. • If possible, different strategy options with cost estimations are presented and the best one is approved • Organizations and process relevant for the survival and continuity need to have a Business Impact Assessment (BIA). The BIA evaluates critical deliverables, dependencies, classifications, established measures. It can initiate more detailed risk assessments and additional protective measures. • An escalation pass with decision point has been established and tested; who can declare a major disruption and what happens then • Detailed business Continuity procedures are available and kept up to date • External and Third Parties and their personal that are crucial for the continuity are involved, informed and trained. If they have own continuity precautions, the interaction is ensured, ideally tested regularly • The communication and actions of when and how a to operate following the contingency plan has been defined and tested • Business Continuity engages with IT Continuity and IT Disaster Recovery measures (Disaster Recovery Plan). Outage and recovery timelines are defined in the DRP. • The backup frequencies, types, medias etc. for information in all forms are defined resp. references to back up plan are established • The Plan and the Strategy is approved by senior management and affected business representatives • Organizational and technical continuity measures and the necessary resources are defined; e.g. a manual workaround can be establishing until the affected system has been replaced	COBIT 5 Processes: DSS04.01 Define the business continuity policy, DSS04.02 Maintain a continuity strategy, DSS04.03 Develop and implement a business continuity response, DSS04.05 Review, maintain and improve the continuity plan, DSS04.07 Manage backup arrangements PCI DSS 3.2: 12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the

• A secure location to operate during the crises e.g. a “Emergency Command Center” is set up, the location is known to the relevant roles in the BCP • The relevant documentation and resources are stored secure e.g. in an Emergency Command Center • Procedures and conditions to evaluate data integrity in the systems and databases are defined • A final testing and approval is needed to declare the end of the disruption and allow business as usual operations of all processes and systems	event [more]
Evidence / Finding	**Auditor/ Assessor**
Mandatory. Auditor or Assessor enters his finding or evidence that was presented. Attachments can be added online, they are not part of the report.	Heike Klaus
Management Response (optional) Optional field. This is an essential field to collect statements or justifications from management, stakeholders for a specific control finding.	

Section only displayed if used!

Action item ID	Person Responsible	Agreed Completion Date
6 Action item to address a finding / impro...	Action User	2019-03-28

Action item to address a finding / improvement for a specific control.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Reviewer Comment
Optional field. Reviewer comments. Text, maximum of 1000 characters allowed.

Control Domain	Control	Control Area	Control ID	Status
Business Continuity Management	Geographical distance has to be considered for Disaster Recovery Sites (e.g. for hosted applications)	Procedures & Processes	BC02.0005	Passed

Control Requirements	Covered Standards
Geographical distance between Disaster Recovery Sites needs to be considered. The following requirements have to be taken into consideration for Disaster Recovery Sites (DRS): • DRS has a different risk profile to the main site • DRS has to be located in an area with good accessibility and good infrastructure, e.g. well connected air links, quality train links, comprehensive road systems, good connections from public transportation (airport, railway station) and hotels.	ISO 27001:2013: A12.3.1 Information backup ISO 27002:2013: 12.3.1 Information backup

Evidence / Finding	Auditor/ Assessor
Mandatory. Auditor or Assessor enters his finding or evidence that was presented. Attachments can be added online, they are not part of the report.	Heike Klaus

Management Response (optional)	Agreed.	

Control Domain	Control	Control Area	Control ID	Status
Business Continuity Management	IT Business Continuity Plan is available and up to date.	Procedures & Processes	BC02.0008	Passed - Restrictions

Control Requirements	Covered Standards
An IT Business Continuity Plan (IT BCP) is required for organizations where the continued availability of IT people and IT supporting processes is considered as vital for the continuation of the business. The following aspects need to be implemented as a minimum:	COBIT 5 Processes: DSS04.02 Maintain a continuity strategy ISO 27001:2013: A6.2.2 Teleworking, A12.2.1 Controls against

• IT BCP is up to date and approved by the respective role(s) • IT BCP review cycles are defined and followed • Classification for IT Systems and Information is defined • Activities to recover from malware attacks, including all necessary data and software backup and recovery arrangements • IT Business Continuity Manager is assigned • Recovery Point Objective (RPO), Recovery Time Objective (RTO) and Recovery Consistency Objective (RCO)	malware ISO 27002:2013: 12.2.1 Controls against malware, 6.2.2 Teleworking

Evidence / Finding	**Auditor/ Assessor**
Mandatory. Auditor or Assessor enters his finding or evidence that was presented. Attachments can be added online, they are not part of the report.	Heike Klaus

Action item ID	Person Responsible	Agreed Completion Date
7 Update role description for BCM.	Action User	2019-02-28
Update role description for BCM.		

Control Domain	**Control**	**Control Area**	**Control ID**	**Status**
Business Continuity Management	Management reviews of the Business Continuity Plan and Organization.	Procedures & Processes	BC02.0009	Work in Progress

Control Requirements	**Covered Standards**
Regular documented management reviews of the plan are performed to ensure • Ongoing alignment with the business requirements (operational and strategic objectives) • Consider major changes to the organization and its environment (merger, regulations etc.) • Effectiveness of the testing activities • Continuous improvement activities are executed	COBIT 5 Processes: DSS04.05 Review, maintain and improve the continuity plan ISO 27001:2013: A6.2.2 Teleworking, A12.2.1 Controls against

• Review Business Impact Assessments, evaluate if they need to be updated • If necessary initiate changes to the organization, the BCM set up, policies, testing etc.	malware ISO 27002:2013: 12.2.1 Controls against malware, 6.2.2 Teleworking
Evidence / Finding	**Auditor/ Assessor**
	Heike Klaus

Control Domain	Control	Control Area	Control ID	Status
Business Continuity Management	Communication and training of IT Disaster Recovery Plan (DRP).	Organisation & Training	BC03.0004	Work in Progress
Control Requirements				**Covered Standards**
IT Disaster Recovery Plan (DRP) is communicated to the organization and training is performed based on relevant roles. • Communication/Deployment Plan • Roles and Responsibilities • Training				COBIT 5 Processes: DSS04.07 Manage backup arrangements
Evidence / Finding				**Auditor/ Assessor**
				Heike Klaus

Control Domain	Control	Control Area	Control ID	Status
Business Continuity Management	Coordinator for IT Disaster Recovery is defined and in place.	Organisation & Training	BC03.0005	Work in Progress
Control Requirements				**Covered Standards**

The role of the IT Disaster Recovery coordinator is implemented (based on the size/set up of the company it can also be that several people are assigned to this role). The Disaster Recovery coordinators key accountabilities are: • To facilitate the development and maintenance of the IT Disaster Recovery Plans • To maintain the list of IT critical associates (in alignment with the IT Pandemic Plan Business Critical Position holders or independent list) • To ensure that involved roles in IT Disaster Recovery are trained appropriately • To initiate and coordinate disaster recovery testing	
Evidence / Finding	**Auditor/ Assessor**
	Heike Klaus

• Includes physical location changes especially changes in jurisdiction(s) • Cover changes to subcontracting Internal audit should verify this process reviewing some samples at least every year.	
Evidence / Finding	**Auditor/ Assessor**
	Andy von Grebmer

Control Domain	Control	Control Area	Control ID	Status
Service Provider Management	Third party and supplier selection process.	Procedures & Processes	SP02.0003	Work in Progress
Control Requirements				**Covered Standards**
The organization maintains a fair and transparent third party and supplier selection process. The process • Has a defined owner and at least one deputy • Defined triggers (time and circumstances) for updating the strategy • Includes Request for Information (RFI) and request for Proposal (RFP) • Ensures structured reviews of all RFIs, RFPs and third-party responses • Ensures adequate documentation of requirements with a clarification process (incl. data privacy, PCI, GxP etc.) • Ensures requirement updates during evaluation phase from potential contract partners • Makes evaluation, decision (e.g. contract) and communication process clear to all stakeholders • Creates documented evidence (records with defined retention period) • Outlines timelines e.g. for reviews, milestones, payments • Ensures back ground checks for new third parties • Ensure adequate safeguards and clarification especially for certain contract types like software development (licensing, ownership, escrow agreement etc.) and acquisitions (include service levels,				COBIT 5 Processes: APO10.02 Select suppliers, BAI03.03 Develop solution components, BAI09.03 Manage the asset life cycle, DSS01.02 Manage outsourced IT services, MEA02.01 Monitor internal controls PCI DSS 3.2: 12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to

maintenance procedures, access controls, security, performance review, basis for payment (follow financial approval process) and arbitration procedures etc.) • Clarification of intellectual property rights in accordance with the relevant laws • Consider legal advice regarding ownership and other contractual agreements	engagement.
Evidence / Finding	**Auditor/ Assessor**
	Andy von Grebmer