GdR BI 263

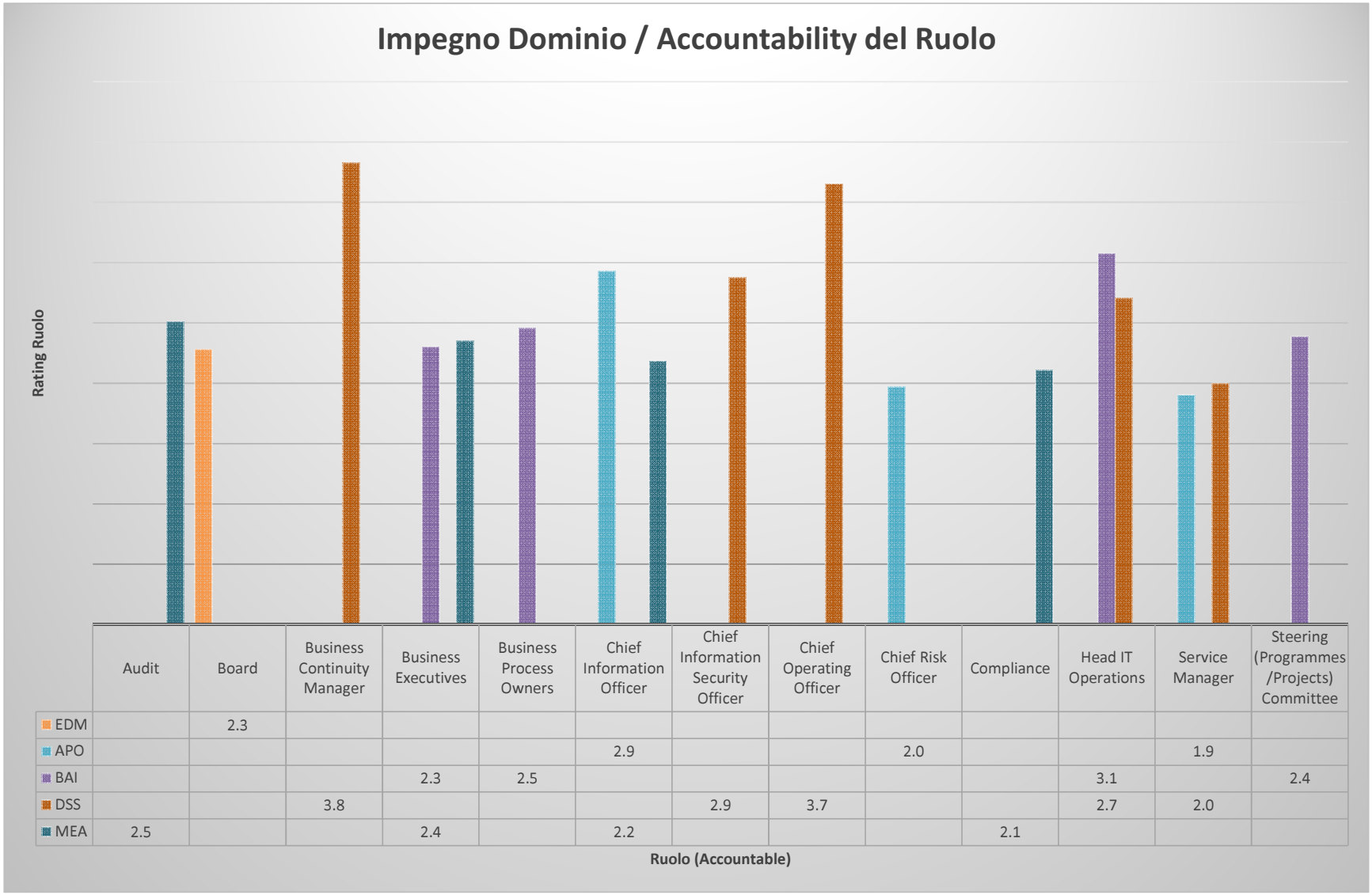
TITOLO V - Capitolo 9 - LA CONTINUITÀ OPERATIVA

Mappatura COBIT®5

Elenco per Accountability

Alessandro Bozzoli, Fabrizio Bulgarelli, Giancarlo Butti, Luca Fei, Valentina Iuvara, Alberto Piamonte,Denis Piazzi,Natale Prampolini, Emanuele Romeo, Ugo Vignolo Lutati

Impegno per Ruolo



	Audit	Board	Business Continuity Manager	Business Executives	Business Process Owners	Chief Information Officer	Chief Information Security Officer	Chief Operating Officer	Chief Risk Officer	Compliance	Head IT Operations	Service Manager	Steering (Programmes /Projects) Committee
EDM		2.3											
APO						2.9			2.0			1.9	
BAI				2.3	2.5						3.1		2.4
DSS			3.8				2.9	3.7			2.7	2.0	
MEA	2.5			2.4		2.2				2.1			

Board

EDM05 - Ensure Stakeholder Transparency

(Rating per ruolo :2.3)

Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.

Purpose

Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's strategy.

Process Outcomes (Goals)
1. Stakeholder reporting is in line with stakeholder requirements.
2. Reporting is complete, timely and accurate.
3. Communication is effective and stakeholders are satisfied.

EDM05.01 - Evaluate stakeholder reporting requirements. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	**from**
Actions to improve value delivery	**Board (EDM02.03)**
Risk management issues for the board	**Board (EDM03.03)**
Feedback on allocation and effectiveness of resources and capabilities	**Board (EDM04.03)**
Refined scope	**Audit (MEA02.08)**

Output	**to**
Evaluation of enterprise reporting requirements	**Chief Executive Officer (MEA01.01)**
Reporting and communication principles	**Chief Executive Officer (MEA01.01)**

Activities

Activity	Peso
S.2. Identify requirements for reporting on information security to stakeholders (e.g., what information is required, when it is required, how it is presented).	**2.0**

Altri responsabili

Chief Executive Officer, Chief Information Officer

EDM05.02 - Direct stakeholder communication and reporting. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
Risk analysis and risk profile reports for stakeholders	**Chief Information Officer (APO12.04)**

Output	to
Rules for validating and approving mandatory reports	**Chief Executive Officer (MEA01.01), Audit (MEA03.04)**
Escalation guidelines	**Chief Information Officer (MEA01.05)**

Activities

Activity	Peso
S.3. Produce for stakeholders regular information security status reports that include information security activities, performance, achievements, risk profile, business benefits, 'hot topics' (e.g., cloud, consumer products), outstanding risk (including compliance and audit) and capability gaps.	**2.0**

Altri responsabili

Chief Executive Officer, Chief Information Officer

Chief Operating Officer

DSS04 - Manage Continuity

(Rating per ruolo :3.7)

Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

Purpose

Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

Process Outcomes (Goals)
1. Business-critical information is available to the business in line with minimum required service levels.
2. Sufficient resilience is in place for critical services.
3. Service continuity tests have verified the effectiveness of the plan.
4. An up-to-date continuity plan reflects current business requirements.
5. Internal and external parties have been trained in the continuity plan.

DSS04.01 - Define the business continuity policy, objectives and scope. (Rating per ruolo :3.1)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	**Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)**
9.I.4	**Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)**
9.A.I.1	**Premessa**
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
SLAs	**Service Manager (APO09.03)**

Output	to
Policy and objectives for business continuity	**Chief Executive Officer (APO01.04)**
Disruptive incident scenarios	**(Internal)**
Assessments of current continuity capabilities and gaps	**(Internal)**

Activities

Activity	Peso
B.1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/ or contractual obligations.	**2.6**
B.2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	**2.6**
B.3. Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the enterprise culture.	**2.4**
B.4. Identify essential supporting business processes and related IT services.	**2.5**

Altri responsabili

Business Process Owners, Chief Information Officer, Head IT Operations, Service Manager, Business Continuity Manager

DSS04.02 - Maintain a continuity strategy. (Rating per ruolo :3.3)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	**Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)**
9.I.4	**Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)**
9.A.I.1	**Premessa**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
• Risk-related root causes • Risk impact communications	**Chief Information Officer (APO12.06)**

Output	to
Business impact analyses	Chief Information Officer (APO12.02)
Continuity requirements	(Internal)
Approved strategic options	Chief Information Officer (APO02.05)

Activities

Activity	Peso
B.1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	2.2
B.2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.	2.3
B.3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage.	2.7
B.4. Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	2.4
B.5. Analyse continuity requirements to identify the possible strategic business and technical options.	2.2
B.6. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	2.5
B.7. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.	2.6
B.8. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	2.2
B.9. Obtain executive business approval for selected strategic options.	2.0

Altri responsabili

Business Process Owners, Chief Information Officer, Head Architect, Head IT Operations, Business Continuity Manager

DSS04.05 - Review, maintain and improve the continuity plan. (Rating per ruolo :3.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)
9.I.4	Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)
9.A.II.3	Definizione del piano di continuità operativa e gestione delle crisi
9.A.III.2	Definizione del piano di continuità operativa e gestione delle crisi
9.A.III.3	Comunicazioni alla Banca d'Italia

Inputs & Outputs

Output	to
Results of reviews of plans	**(Internal)**
Recommended changes to plans	**(Internal)**

Activities

Activity	Peso
B.1. Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.	**2.5**
B.2. Consider whether a revised business impact assessment may be required, depending on the nature of the change.	**2.2**
B.3. Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.	**2.5**
B.4. Review the continuity plan on a regular basis to consider the impact of new or major changes to: enterprise organisation, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.	**2.5**

Altri responsabili

Business Process Owners, Chief Information Officer, Head IT Operations, Business Continuity Manager

Business Executives

BAI06 - Manage Changes

(Rating per ruolo :2.3)

Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.

Purpose

Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

Process Outcomes (Goals)
1. Authorised changes are made in a timely manner and with minimal errors.
2. Impact assessments reveal the effect of the change on all affected components.
3. All emergency changes are reviewed and authorised after the change.
4. Key stakeholders are kept informed of all aspects of the change.

BAI06.01 - Evaluate, prioritise and authorise change requests. (Rating per ruolo :1.9)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	**from**
Integrated and configured solution components	**Head Development (BAI03.05)**
Approved service requests	**Service Manager (DSS02.03)**
Proposed solutions to known errors	**Head IT Operations (DSS03.03)**
Identified sustainable solutions	**Service Manager (DSS03.05)**
Approved changes to the plans	**Business Continuity Manager (DSS04.08)**
Root cause analyses and recommendations	**Business Executives (DSS06.01)**

Output	to
Impact assessments	**(Internal)**
Approved requests for change	**Steering (Programmes/Projects) Committee (BAI07.01)**
Change plan and schedule	**Steering (Programmes/Projects) Committee (BAI07.01)**

Activities

Activity	Peso
B.4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.	**1.9**

Altri responsabili

Business Process Owners, Chief Information Officer, Head Development, Head IT Operations, Service Manager

BAI06.04 - Close and document the changes. (Rating per ruolo :2.1)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Change documentation	**(Internal)**

Activities

Activity	Peso
B.1. Include changes to documentation (e.g., business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials) within the change management procedure as an integral part of the change.	**2.1**

Altri responsabili

Business Process Owners, Project Management Office, Chief Information Officer, Head Development, Head IT Operations

MEA01 - Monitor, Evaluate and Assess Performance and Conformance

(Rating per ruolo :2.4)

Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.

Purpose

Provide transparency of performance and conformance and drive achievement of goals.

Process Outcomes (Goals)
1. Goals and metrics are approved by the stakeholders.
2. Processes are measured against agreed-on goals and metrics.
3. The enterprise monitoring, assessing and informing approach is effective and operational.
4. Goals and metrics are integrated within enterprise monitoring systems.
5. Process reporting on performance and conformance is useful and timely.

MEA01.04 - Analyse and report performance. (Rating per ruolo :2.4)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	**to**
Performance reports	**Board (EDM01.03), (All APO), (All BAI), (All DSS), (All MEA)**

Activities

Activity	Peso
B.1. Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports) and ensure that the cause and effect between goals and metrics are communicated in an understandable manner.	**1.6**
B.2. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors).	**1.6**
B.3. Recommend changes to the goals and metrics, where appropriate.	**1.6**
B.4. Distribute reports to the relevant stakeholders.	**1.6**
B.5. Analyse the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Document results.	**1.6**
B.6. Where feasible, link achievement of performance targets to the organisational reward compensation system.	**1.6**

Altri responsabili

Business Process Owners, Head Development, Head IT Operations, Service Manager

Business Process Owners

BAI04 - Manage Availability and Capacity

(Rating per ruolo :2.5)

Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.

Purpose

Maintain service availability, efficient management of resources, and optimisation of system performance through prediction of future performance and capacity requirements.

Process Outcomes (Goals)
1. The availability plan anticipates the business expectation of critical capacity requirements.
2. Capacity, performance and availability meet requirements.
3. Availability, performance and capacity issues are identified and routinely resolved.

BAI04.02 - Assess business impact. (Rating per ruolo :2.5)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.2	**Analisi di impatto**

Inputs & Outputs

Input	**from**
Internal and external SLAs	**Head Development (BAI03.02)**

Output	**to**
Availability, performance and capacity scenarios	**(Internal)**
Availability, performance and capacity business impact assessments	**(Internal)**

Activities

Activity	Peso
B.1. Identify only those solutions or services that are critical in the availability and capacity management process.	**1.5**
B.2. Map the selected solutions or services to application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.	**1.5**
B.3. Collect data on availability patterns from logs of past failures and performance monitoring. Use modelling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.	**2.0**
B.4. Create scenarios based on the collected data, describing future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.	**1.5**
B.5. Determine the likelihood that the availability performance objective will not be achieved based on the scenarios.	**1.5**
B.6. Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business line, functional (especially finance) and regional leaders to understand their evaluation of impact.	**1.5**
B.7. Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.	**1.5**

Altri responsabili

Head IT Operations, Service Manager

Steering (Programmes/Projects) Committee

BAI02 - Manage Requirements Definition

(Rating per ruolo :2.3)

Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinate with affected stakeholders the review of feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.

Purpose

Create feasible optimal solutions that meet enterprise needs while minimising risk.

Process Outcomes (Goals)
1. Business functional and technical requirements reflect enterprise needs and expectations.
2. The proposed solution satisfies business functional, technical and compliance requirements.
3. Risk associated with the requirements has been addressed in the proposed solution.
4. Requirements and proposed solutions meet business case objectives (value expected and likely costs).

BAI02.01 - Define and maintain business functional and technical requirements. (Rating per ruolo :2.3)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
• Data integrity procedures • Data security and control guidelines • Data classification guidelines	**Business Executives (APO01.06)**
Architecture principles	**Chief Executive Officer (APO03.01)**
• Information architecture model • Baseline domain descriptions and architecture definition	**Architecture Board (APO03.02)**
Solution development guidance	**Chief Executive Officer (APO03.05)**
Supplier RFIs and RFPs	**Chief Information Officer (APO10.02)**
Acceptance criteria	**Business Executives (APO11.03)**

Output	to
Requirements definition repository	**Head Development (BAI03.01), Head Development (BAI03.02), Head IT Operations (BAI04.01), Chief Executive Officer (BAI05.01)**
Confirmed acceptance criteria from stakeholders	**Head Development (BAI03.01), Head Development (BAI03.02), Head IT Operations (BAI04.03), Chief Executive Officer (BAI05.01), Business Executives (BAI05.02)**
Record of requirement change requests	**Steering (Programmes/Projects) Committee (BAI03.09)**

Activities

Activity	Peso
B.6. Confirm acceptance of key aspects of the requirements, including enterprise rules, information controls, business continuity, legal and regulatory compliance, auditability, ergonomics, operability and usability, safety, and supporting documentation.	**2.3**

Altri responsabili

Business Process Owners, Project Management Office, Head Architect, Head Development

BAI07 - Manage Change Acceptance and Transitioning

(Rating per ruolo :1.5)

Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review.

Purpose

Implement solutions safely and in line with the agreed-on expectations and outcomes.

Process Outcomes (Goals)
1. Acceptance testing meets stakeholder approval and takes into account all aspects of the implementation and conversion plans.
2. Releases are ready for promotion into production with stakeholder readiness and support.
3. Releases are promoted successfully, are stable and meet expectations.
4. Lessons learned contribute to future releases.

BAI07.02 - Plan business process, system and data conversion. (Rating per ruolo :1.5)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Migration plan	**Business Executives (DSS06.02)**

Activities

Activity	Peso
B.6. Consider the risk of conversion problems, business continuity planning, and fallback procedures in the business process, data and infrastructure migration plan where there are risk management, business needs or regulatory/compliance requirements.	**1.5**

Altri responsabili

Business Process Owners, Chief Risk Officer, Chief Information Officer, Head Development, Service Manager, Information Security Manager, Business Continuity Manager

Chief Risk Officer

APO12 - Manage Risk

(Rating per ruolo :2.0)

Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Purpose

Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

Process Outcomes (Goals)
1. IT-related risk is identified, analysed, managed and reported.
2. A current and complete risk profile exists.
3. All significant risk management actions are managed and under control.
4. Risk management actions are implemented effectively.

APO12.03 - Maintain a risk profile. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	**from**
• Approved risk tolerance levels • Risk appetite guidance	**Board (EDM03.01)**
Identified supplier delivery risk	**Chief Information Officer (APO10.04)**
Evaluations of potential threats	**Chief Information Security Officer (DSS05.01)**

Output	**to**
Documented risk scenarios by line of business and function	**(Internal)**
Aggregated risk profile, including status of risk management actions	**Board (EDM03.02), Chief Information Officer (APO02.02)**

Activities

Activity	Peso
B.1. Inventory business processes, including supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers, and document the dependency on IT service management processes and IT infrastructure resources.	**1.1**
B.2. Determine and agree on which IT services and IT infrastructure resources are essential to sustain the operation of business processes. Analyse dependencies and identify weak links.	**1.1**
B.3. Aggregate current risk scenarios by category, business line and functional area.	**1.1**
B.4. On a regular basis, capture all risk profile information and consolidate it into an aggregated risk profile.	**1.1**
B.5. Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	**1.1**
B.6. Capture information on IT risk events that have materialised, for inclusion in the IT risk profile of the enterprise.	**1.1**
B.7. Capture information on the status of the risk action plan, for inclusion in the IT risk profile of the enterprise.	**1.1**

Altri responsabili

Business Process Owners, Compliance, Audit, Chief Information Officer

Chief Information Security Officer

DSS01 - Manage Operations

(Rating per ruolo :2.9)

Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.

Purpose

Deliver IT operational service outcomes as planned.

Process Outcomes (Goals)
1. Operational activities are performed as required and scheduled.
2. Operations are monitored, measured, reported and remediated.

DSS01.04 - Manage the environment. (Rating per ruolo :2.4)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Environmental policies	**Chief Executive Officer (APO01.08)**
Insurance policy reports	**Compliance (MEA03.03)**

Activities

Activity	Peso
B.1. Identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities.	**2.2**
B.3. Situate and construct IT facilities to minimise and mitigate susceptibility to environmental threats.	**2.0**

Altri responsabili

Head IT Operations, Information Security Manager

DSS01.05 - Manage facilities. (Rating per ruolo :2.7)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.1	**Ambito del piano di continuità operativa**

Inputs & Outputs

Output	to
Facilities assessment reports	**Chief Information Officer (MEA01.03)**
Health and safety awareness	**(Internal)**

Activities

Activity	Peso
B.1. Examine the IT facilities' requirement for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.	**1.6**
B.2. Regularly test the uninterruptible power supply's mechanisms, and ensure that power can be switched to the supply without any significant effect on business operations.	**1.6**
B.3. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.	**1.6**
B.4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorised personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.	**1.6**
B.5. Ensure that cabling and physical patching (data and phone) are structured and organised. Cabling and conduit structures should be documented (e.g., blueprint building plan and wiring diagrams).	**1.6**
B.6. Analyse the facilities housing's high-availability systems for redundancy and fail-over cabling requirements (external and internal).	**1.6**
B.7. Ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.	**1.6**
B.8. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.	**1.6**
B.9. Record, monitor, manage and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations.	**1.6**
B.10. Ensure that IT sites and equipment are maintained according to the supplier's recommended service intervals and specifications. The maintenance must be carried out only by authorised personnel.	**1.6**
B.11. Analyse physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.	**1.6**

Altri responsabili

Head IT Operations, Information Security Manager

Compliance

MEA02 - Monitor, Evaluate and Assess the System of Internal Control

(Rating per ruolo :1.5)

Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.

Purpose

Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

Process Outcomes (Goals)
1. Processes, resources and information meet enterprise internal control system requirements.
2. All assurance initiatives are planned and executed effectively.
3. Independent assurance that the system of internal control is operational and effective is provided.
4. Internal control is established and deficiencies are identified and reported.

MEA02.05 - Ensure that assurance providers are independent and qualified. (Rating per ruolo :1.5)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Activities

Activity	Peso
B.1. Establish adherence to applicable codes of ethics and standards (e.g., Code of Professional Ethics of ISACA) and (industry- and geography-specific) assurance standards, e.g., IT Audit and Assurance Standards of ISACA and the International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework).	**1.0**
B.2. Establish independence of assurance providers.	**1.0**
B.3. Establish competency and qualification of assurance providers.	**1.0**

Altri responsabili

Business Process Owners, Chief Information Officer

MEA03 - Monitor, Evaluate and Assess Compliance with External Requirements

(Rating per ruolo :2.0)

Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

Purpose

Ensure that the enterprise is compliant with all applicable external requirements.

Process Outcomes (Goals)
1. All external compliance requirements are identified.
2. External compliance requirements are adequately addressed.

MEA03.03 - Confirm external compliance. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Compliance audit results	**Business Executives (BAI05.06)**
Results of installed licence audits	**Chief Information Officer (BAI09.05)**
Licence deviations	**Head IT Operations (BAI10.05)**
Insurance policy reports	**Chief Information Security Officer (DSS01.04)**

Output	to
Identified compliance gaps	**Audit (MEA02.08)**
Compliance confirmations	**Board (EDM01.03)**

Activities

Activity	Peso
B.1. Regularly evaluate organisational policies, standards, procedures and methodologies in all functions of the enterprise to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.	**1.4**
B.2. Address compliance gaps in policies, standards and procedures on a timely basis.	**1.4**
B.3. Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.	**1.4**
B.4. Regularly review for recurring patterns of compliance failures. Where necessary, improve policies, standards, procedures, methodologies, and associated processes and activities.	**1.4**

Altri responsabili

Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Business Executives, Business Process Owners, Chief Information Officer, Privacy Officer

Audit

MEA02 - Monitor, Evaluate and Assess the System of Internal Control

(Rating per ruolo :2.2)

Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.

Purpose

Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

Process Outcomes (Goals)
1. Processes, resources and information meet enterprise internal control system requirements.
2. All assurance initiatives are planned and executed effectively.
3. Independent assurance that the system of internal control is operational and effective is provided.
4. Internal control is established and deficiencies are identified and reported.

MEA02.05 - Ensure that assurance providers are independent and qualified. (Rating per ruolo :1.5)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Activities

Activity	Peso
B.1. Establish adherence to applicable codes of ethics and standards (e.g., Code of Professional Ethics of ISACA) and (industry- and geography-specific) assurance standards, e.g., IT Audit and Assurance Standards of ISACA and the International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework).	**1.0**
B.2. Establish independence of assurance providers.	**1.0**
B.3. Establish competency and qualification of assurance providers.	**1.0**

Altri responsabili

Business Process Owners, Chief Information Officer

MEA02.08 - Execute assurance initiatives. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Root causes of quality delivery failures	**Chief Information Officer (APO11.05)**
Risk analysis and risk profile reports for stakeholders	**Chief Information Officer (APO12.04)**
Risk-related root causes	**Chief Information Officer (APO12.06)**
Results of penetration tests	**Chief Information Security Officer (DSS05.02)**
Root cause analyses and recommendations	**Business Executives (DSS06.01)**
Identified compliance gaps	**Compliance (MEA03.03)**

Output	to
Refined scope	**(All APO), (All BAI), (All DSS), (All MEA)**
Assurance review results	**Board (EDM05.01), Board (EDM05.03), (All APO), (All BAI), (All DSS), (All MEA)**
Assurance review report	**Board (EDM05.03), (All APO), (All BAI), (All DSS), (All MEA)**

Activities

Activity	Peso
B.3. Test the effectiveness of the control design of the key control objectives.	**1.7**
B.4. Alternatively/additionally test the outcome of the key control objectives.	**1.7**

Altri responsabili

Business Process Owners, Chief Information Officer

MEA03 - Monitor, Evaluate and Assess Compliance with External Requirements

(Rating per ruolo :2.3)

Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

Purpose

Ensure that the enterprise is compliant with all applicable external requirements.

Process Outcomes (Goals)
1. All external compliance requirements are identified.
2. External compliance requirements are adequately addressed.

MEA03.04 - Obtain assurance of external compliance. (Rating per ruolo :2.3)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Rules for validating and approving mandatory reports	**Board (EDM05.02)**
Assessment of reporting effectiveness	**Board (EDM05.03)**

Output	to
Compliance assurance reports	**Board (EDM01.03)**
Reports of non-compliance issues and root causes	**Board (EDM01.03), Audit (MEA02.07)**

Activities

Activity	Peso
B.1. Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.	**1.6**
B.2. Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.	**1.6**
B.3. If required, obtain assertions from third-party IT service providers on levels of their compliance with applicable laws and regulations.	**1.6**
B.4. If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.	**1.6**
B.5. Monitor and report on non-compliance issues and, where necessary, investigate the root cause.	**1.6**
B.6. Integrate reporting on legal, regulatory and contractual requirements at an enterprisewide level, involving all business units.	**1.6**

Altri responsabili

Chief Information Officer

Alessandro Bozzoli, Fabrizio Bulgarelli, Giancarlo Butti, Luca Fei, Valentina Iuvara, Alberto Piamonte,Denis Piazzi,Natale Prampolini, Emanuele Romeo, Ugo Vignolo Lutati

Chief Information Officer

APO01 - Manage the IT Management Framework

(Rating per ruolo :2.3)

Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies.

Purpose

Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies.

Process Outcomes (Goals)
1. An effective set of policies is defined and maintained.
2. Everyone is aware of the policies and how they should be implemented.

APO01.02 - Establish roles and responsibilities. (Rating per ruolo :2.3)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	**Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)**
9.I.4	**Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)**

Inputs & Outputs

Input	from
Authority levels	**Board (EDM01.01)**
Assigned responsibilities for resource management	**Board (EDM04.02)**
• Skill development plans • Skills and competencies matrix	**Chief Information Officer (APO07.03)**
Quality management system (QMS) roles, responsibilities and decision rights	**Chief Operating Officer (APO11.01)**
Information security management system (ISMS) scope statement	**Chief Information Security Officer (APO13.01)**
• Allocated levels of authority • Allocated roles and responsibilities	**Business Executives (DSS06.03)**

Output	to
Definition of IT-related roles and responsibilities	**Chief Information Security Officer (DSS05.04)**
Definition of supervisory practices	**Chief Information Officer (APO07.01)**

Activities

Activity	Peso
B.1. Establish, agree on and communicate IT-related roles and responsibilities for all personnel in the enterprise, in alignment with business needs and objectives. Clearly delineate responsibilities and accountabilities, especially for decision making and approvals.	**1.8**
B.2. Consider requirements from enterprise and IT service continuity when defining roles, including staff back-up and cross-training requirements.	**1.8**
B.3. Provide input to the IT service continuity process by maintaining up-to-date contact information and role descriptions in the enterprise.	**1.8**

Altri responsabili

Head IT Administration

APO02 - Manage Strategy

(Rating per ruolo :1.8)

Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives.

Purpose

Align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans.

Process Outcomes (Goals)
1. All aspects of the IT strategy are aligned with the enterprise strategy.
2. The IT strategy is cost-effective, appropriate, realistic, achievable, enterprise-focussed and balanced.
3. Clear and concrete short-term goals can be derived from, and traced back to, specific long-term initiatives, and can then be translated into operational plans.
4. IT is a value driver for the enterprise.
5. There is awareness of the IT strategy and a clear assignment of accountability for delivery.

APO02.02 - Assess the current environment, capabilities and performance. (Rating per ruolo :1.8)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	Comunicazioni alla Banca d'Italia

Inputs & Outputs

Input	from
Cost optimisation opportunities	Chief Information Officer (APO06.05)
Definition of potential improvement projects	Chief Information Officer (APO08.05)
Identified gaps in IT services to the business	Service Manager (APO09.01)
Improvement action plans and remediations	Service Manager (APO09.04)
Emerging risk issues and factors	Chief Information Officer (APO12.01)
Risk analysis results	Chief Information Officer (APO12.02)
Aggregated risk profile, including status of risk management actions	Chief Risk Officer (APO12.03)
Project proposals for reducing risk	Chief Risk Officer (APO12.05)
• Performance and capacity plans • Prioritised improvements	Head IT Operations (BAI04.03)
Corrective actions	Head IT Operations (BAI04.05)
Results of fit-for-purpose reviews	Head IT Operations (BAI09.01)
• Opportunities to reduce asset costs or increase value • Results of cost optimisation reviews	Chief Information Officer (BAI09.04)

Output	to
Baseline of current capabilities	(Internal)
Gaps and risk related to current capabilities	Chief Information Officer (APO12.01)
Capability SWOT analysis	(Internal)

Activities

Activity	Peso
B.1. Develop a baseline of the current business and IT environment, capabilities and services against which future requirements can be compared. Include the relevant high-level detail of the current enterprise architecture (business, information, data, applications and technology domains), business processes, IT processes and procedures, the IT organisation structure, external service provision, governance of IT, and enterprisewide IT related skills and competencies.	1.2
B.2. Identify risk from current, potential and declining technologies.	1.2
B.3. Identify gaps between current business and IT capabilities and services and reference standards and best practices, competitor business and IT capabilities, and comparative benchmarks of best practice and emerging IT service provision.	1.2
B.4. Identify issues, strengths, opportunities and threats in the current environment, capabilities and services to understand current performance. Identify areas for improvement in terms of IT's contribution to enterprise objectives.	1.2

Altri responsabili

Business Executives, Head Architect, Head Development, Head IT Operations

APO07 - Manage Human Resources

(Rating per ruolo :2.0)

Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.

Purpose

Optimise human resources capabilities to meet enterprise objectives.

Process Outcomes (Goals)
1. The IT organisational structure and relationships are flexible and responsive.
2. Human resources are effectively and efficiently managed.

APO07.02 - Identify key IT personnel. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Activities

Activity	Peso
B.1. Minimise reliance on a single individual performing a critical job function through knowledge capture (documentation), knowledge sharing, succession planning, staff backup, cross-training and job rotation initiatives.	**1.8**
B.2. As a security precaution, provide guidelines on a minimum time of annual vacation to be taken by key individuals.	**1.1**
B.3. Take expedient actions regarding job changes, especially job terminations.	**1.1**
B.4. Regularly test staff backup plans.	**1.1**

Altri responsabili

Project Management Office, Head Human Resources, Head Architect, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager

APO10 - Manage Suppliers

(Rating per ruolo :2.0)

Manage IT-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.

Purpose

Minimise the risk associated with non-performing suppliers and ensure competitive pricing.

Process Outcomes (Goals)
1. Suppliers perform as agreed.
2. Supplier risk is assessed and properly addressed.
3. Supplier relationships are working effectively.

APO10.01 - Identify and evaluate supplier relationships and contracts. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.1	**Ambito del piano di continuità operativa**

Inputs & Outputs

Input	**from**
Supplier contracts	**(Outside COBIT)**

Output	**to**
Supplier significance and evaluation criteria	**(Internal)**
Supplier catalogue	**Steering (Programmes/Projects) Committee (BAI02.02)**
Potential revisions to supplier contracts	**(Internal)**

Activities

Activity	**Peso**
B.1. Establish and maintain criteria relating to type, significance and criticality of suppliers and supplier contracts, enabling a focus on preferred and important suppliers.	**2.0**

Altri responsabili
Head IT Administration

APO12 - Manage Risk

(Rating per ruolo :2.6)

Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Purpose

Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

Process Outcomes (Goals)
1. IT-related risk is identified, analysed, managed and reported.
2. A current and complete risk profile exists.
3. All significant risk management actions are managed and under control.
4. Risk management actions are implemented effectively.

APO12.01 - Collect data. (Rating per ruolo :1.8)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.1	**Ambito del piano di continuità operativa**

Inputs & Outputs

Input	**from**
Evaluation of risk management activities	**Board (EDM03.01)**
• Approved process for measuring risk management • Key objectives to be monitored for risk management • Risk management policies	**Board (EDM03.02)**
Gaps and risk related to current capabilities	**Chief Information Officer (APO02.02)**
Risk assessment	**Chief Information Officer (APO02.05)**
Identified supplier delivery risk	**Chief Information Officer (APO10.04)**
Incident status and trends report	**Head IT Operations (DSS02.07)**

Output	to
Data on the operating environment relating to risk	**(Internal)**
Data on risk events and contributing factors	**(Internal)**
Emerging risk issues and factors	**Board (EDM03.01), Chief Executive Officer (APO01.03), Chief Information Officer (APO02.02)**

Activities

Activity	Peso
B.1. Establish and maintain a method for the collection, classification and analysis of IT risk-related data, accommodating multiple types of events, multiple categories of IT risk and multiple risk factors.	**1.8**

Altri responsabili

Business Process Owners, Project Management Office, Chief Risk Officer, Chief Information Security Officer, Head Architect, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager, Privacy Officer

APO12.02 - Analyse risk. (Rating per ruolo :2.4)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.II.2	**Analisi di impatto**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Business impact analyses	**Chief Operating Officer (DSS04.02)**
Evaluations of potential threats	**Chief Information Security Officer (DSS05.01)**
Threat advisories	**(Outside COBIT)**

Output	to
Scope of risk analysis efforts	**(Internal)**
IT risk scenarios	**(Internal)**
Risk analysis results	**Board (EDM03.03), Chief Executive Officer (APO01.03), Chief Information Officer (APO02.02), Steering (Programmes/Projects) Committee (BAI01.10)**

Activities

Activity	Peso
B.1. Define the appropriate breadth and depth of risk analysis efforts, considering all risk factors and the business criticality of assets. Set the risk analysis scope after performing a cost-benefit analysis.	**1.9**
B.2. Build and regularly update IT risk scenarios, including compound scenarios of cascading and/or coincidental threat types, and develop expectations for specific control activities, capabilities to detect and other response measures.	**2.0**
B.3. Estimate the frequency and magnitude of loss or gain associated with IT risk scenarios. Take into account all applicable risk factors, evaluate known operational controls and estimate residual risk levels.	**1.1**
B.4. Compare residual risk to acceptable risk tolerance and identify exposures that may require a risk response.	**1.1**
B.5. Analyse cost-benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Propose the optimal risk response.	**1.1**
B.6. Specify high-level requirements for projects or programmes that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.	**1.1**
B.7. Validate the risk analysis results before using them in decision making, confirming that the analysis aligns with enterprise requirements and verifying that estimations were properly calibrated and scrutinised for bias.	**1.1**

Altri responsabili

Business Process Owners, Chief Risk Officer, Compliance, Audit

APO12.06 - Respond to risk. (Rating per ruolo :1.9)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
Remedial actions to address risk management deviations	**Board (EDM03.03)**

Output	to
Risk-related incident response plans	**Service Manager (DSS02.05)**
Risk impact communications	**Chief Executive Officer (APO01.04), Chief Information Officer (APO08.04), Chief Operating Officer (DSS04.02)**
Risk-related root causes	**Service Manager (DSS02.03), Service Manager (DSS03.01), Head IT Operations (DSS03.02), Chief Operating Officer (DSS04.02), Chief Information Officer (MEA02.04), Audit (MEA02.07), Audit (MEA02.08)**

Activities

Activity	Peso
B.1. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.	**1.6**
B.4. Examine past adverse events/losses and missed opportunities and determine root causes. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers and ensure that the cause, response requirements and process improvement are included in risk governance processes.	**1.6**

Altri responsabili

Business Process Owners, Project Management Office, Chief Risk Officer, Chief Information Security Officer, Head Architect, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager, Privacy Officer

MEA02 - Monitor, Evaluate and Assess the System of Internal Control

(Rating per ruolo :2.2)

Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.

Purpose

Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

Process Outcomes (Goals)
1. Processes, resources and information meet enterprise internal control system requirements.
2. All assurance initiatives are planned and executed effectively.
3. Independent assurance that the system of internal control is operational and effective is provided.
4. Internal control is established and deficiencies are identified and reported.

MEA02.01 - Monitor internal controls. (Rating per ruolo :1.7)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Results of third-party risk assessments	**Chief Information Officer (APO12.04)**
ISMS audit reports	**Chief Information Security Officer (APO13.03)**
Industry standards and good practices	**(Outside COBIT)**

Output	to
Results of internal control monitoring and reviews	**Board (EDM01.03), (All APO), (All BAI), (All DSS), (All MEA)**
Results of benchmarking and other evaluations	**Board (EDM01.03), (All APO), (All BAI), (All DSS), (All MEA)**

Activities

Activity	Peso
B.7. Assess the status of external service providers' internal controls and confirm that service providers comply with legal and regulatory requirements and contractual obligations.	**1.7**

Altri responsabili

Business Process Owners, Project Management Office, Chief Risk Officer, Compliance, Audit, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager, Privacy Officer

MEA02.04 - Identify and report control deficiencies. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
Root causes of quality delivery failures	Chief Information Officer (APO11.05)
Risk-related root causes	Chief Information Officer (APO12.06)
• Root cause analyses and recommendations • Results of processing effectiveness reviews	Business Executives (DSS06.01)
Evidence of error correction and remediation	Business Process Owners (DSS06.04)

Output	to
Control deficiencies	(All APO), (All BAI), (All DSS), (All MEA)
Remedial actions	(All APO), (All BAI), (All DSS), (All MEA)

Activities

Activity	Peso
B.1. Identify, report and log control exceptions, and assign responsibility for resolving them and reporting on the status.	1.2
B.2. Consider related enterprise risk to establish thresholds for escalation of control exceptions and breakdowns.	1.2
B.3. Communicate procedures for escalation of control exceptions, root cause analysis, and reporting to process owners and IT stakeholders.	1.2
B.4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected process owners and stakeholders.	1.2
B.5. Follow up on all exceptions to ensure that agreed-on actions have been addressed.	1.2
B.6. Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	1.2

Altri responsabili

Business Process Owners, Project Management Office, Compliance, Audit, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager, Privacy Officer

Head IT Operations

BAI04 - Manage Availability and Capacity

(Rating per ruolo :2.9)

Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.

Purpose

Maintain service availability, efficient management of resources, and optimisation of system performance through prediction of future performance and capacity requirements.

Process Outcomes (Goals)
1. The availability plan anticipates the business expectation of critical capacity requirements.
2. Capacity, performance and availability meet requirements.
3. Availability, performance and capacity issues are identified and routinely resolved.

BAI04.01 - Assess current availability, performance and capacity and create a baseline. (Rating per ruolo :2.8)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.2	**Analisi di impatto**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	**from**
Requirements definition repository	**Steering (Programmes/Projects) Committee (BAI02.01)**
Requirements risk register	**Steering (Programmes/Projects) Committee (BAI02.03)**

Output	**to**
Availability, performance and capacity baselines	**(Internal)**
Evaluations against SLAs	**Business Executives (APO09.05)**

Activities

Activity	Peso
B.1. Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilisation, IT capabilities and industry trends.	**2.2**
B.2. Monitor actual performance and capacity usage against defined thresholds, supported where necessary with automated software.	**2.2**
B.3. Identify and follow up on all incidents caused by inadequate performance or capacity.	**2.2**
B.4. Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs, taking into account changes in the environment.	**2.2**

Altri responsabili

Service Manager

BAI04.05 - Investigate and address availability, performance and capacity issues. (Rating per ruolo :2.1)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Performance and capacity gaps	**(Internal)**
Corrective actions	**Chief Information Officer (APO02.02)**
Emergency escalation procedure	**Head IT Operations (DSS02.02)**

Activities

Activity	Peso
B.1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.	**1.8**
B.2. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritisation.	**1.8**

Altri responsabili

Business Process Owners, Head Architect, Service Manager

BAI09 - Manage Assets

(Rating per ruolo :2.6)

Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with licence agreements.

Purpose

Account for all IT assets and optimise the value provided by these assets.

Process Outcomes (Goals)
1. Licences are compliant and aligned with business need.
2. Assets are maintained at optimal levels.

BAI09.02 - Manage critical assets. (Rating per ruolo :2.6)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.II.2	**Analisi di impatto**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Communication of planned maintenance downtime	**Chief Information Officer (APO08.04)**
Maintenance agreements	**(Internal)**

Activities

Activity	Peso
B.1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, SLAs and the configuration management system.	**1.5**
B.2. Monitor performance of critical assets by examining incident trends and, where necessary, take action to repair or replace.	**1.5**
B.3. On a regular basis, consider the risk of failure or need for replacement of each critical asset.	**1.5**
B.4. Maintain the resilience of critical assets by applying regular preventive maintenance, monitoring performance, and, if required, providing alternative and/or additional assets to minimise the likelihood of failure.	**2.0**
B.5. Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.	**1.5**
B.6. Establish maintenance agreements involving third-party access to organisational IT facilities for on-site and off-site activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorisation procedures, to ensure compliance with the organisational security policies and standards.	**2.0**
B.7. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.	**1.5**
B.8. Ensure that remote access services and user profiles (or other means used for maintenance or diagnosis) are active only when required.	**1.5**
B.9. Incorporate planned downtime in an overall production schedule, and schedule the maintenance activities to minimise the adverse impact on business processes.	**1.5**

Altri responsabili

Head Architect, Head Development, Head IT Administration

DSS02 - Manage Service Requests and Incidents

(Rating per ruolo :2.1)

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Purpose

Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

Process Outcomes (Goals)
1. IT-related services are available for use.
2. Incidents are resolved according to agreed-on service levels.
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.

DSS02.02 - Record, classify and prioritise requests and incidents. (Rating per ruolo :1.8)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	Comunicazioni alla Banca d'Italia

Inputs & Outputs

Input	from
SLAs	Service Manager (APO09.03)
Emergency escalation procedure	Head IT Operations (BAI04.05)
• Incident tickets • Asset monitoring rules and event conditions	Head IT Operations (DSS01.03)
Security incident tickets	Chief Information Security Officer (DSS05.07)

Output	to
Incident and service request log	(Internal)
Classified and prioritised incidents and service requests	Chief Information Officer (APO08.03), Service Manager (APO09.04), Chief Information Security Officer (APO13.03)

Activities

Activity	Peso
B.1. Log all service requests and incidents, recording all relevant information so that they can be handled effectively and a full historical record can be maintained.	1.3
B.2. To enable trend analysis, classify service requests and incidents by identifying type and category.	1.3
B.3. Prioritise service requests and incidents based on SLA service definition of business impact and urgency.	1.3

Altri responsabili

Service Manager

DSS02.07 - Track status and produce reports. (Rating per ruolo :1.9)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.3	Comunicazioni alla Banca d'Italia

Inputs & Outputs

Input	from
OLAs	**Service Manager (APO09.03)**
Problem status reports	**Service Manager (DSS03.01)**
Problem resolution reports	**Head IT Operations (DSS03.02)**
Problem resolution monitoring reports	**Service Manager (DSS03.05)**

Output	to
Incident status and trends report	**Chief Information Officer (APO08.03), Service Manager (APO09.04), Chief Information Officer (APO11.04), Chief Information Officer (APO12.01), Chief Information Officer (MEA01.03)**
Request fulfilment status and trends report	**Chief Information Officer (APO08.03), Service Manager (APO09.04), Chief Information Officer (APO11.04), Chief Information Officer (MEA01.03)**

Activities

Activity	Peso
B.1. Monitor and track incident escalations and resolutions and request handling procedures to progress towards resolution or completion.	**1.3**
B.2. Identify information stakeholders and their needs for data or reports. Identify reporting frequency and medium.	**1.3**
B.3. Analyse incidents and service requests by category and type to establish trends and identify patterns of recurring issues, SLA breaches or inefficiencies. Use the information as input to continual improvement planning.	**1.3**
B.4. Produce and distribute timely reports or provide controlled access to online data.	**1.3**

Altri responsabili

Service Manager

DSS04 - Manage Continuity

(Rating per ruolo :2.6)

Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

Purpose

Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

Process Outcomes (Goals)
1. Business-critical information is available to the business in line with minimum required service levels.

2. Sufficient resilience is in place for critical services.
3. Service continuity tests have verified the effectiveness of the plan.
4. An up-to-date continuity plan reflects current business requirements.
5. Internal and external parties have been trained in the continuity plan.

DSS04.07 - Manage backup arrangements. (Rating per ruolo :2.6)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Output	to
Test results of backup data	**(Internal)**

Activities

Activity	Peso
B.1. Back up systems, applications, data and documentation according to a defined schedule, considering: • Frequency (monthly, weekly, daily, etc.) • Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention) • Type of backup (e.g., full vs. incremental) • Type of media • Automated online backups • Data types (e.g., voice, optical) • Creation of logs • Critical end-user computing data (e.g., spreadsheets) • Physical and logical location of data sources • Security and access rights • Encryption	**2.0**
B.2. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.	**1.7**
B.3. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.	**1.7**
B.4. Roll out BCP awareness and training.	**1.7**
B.5. Periodically test and refresh archived and backup data.	**2.0**

Altri responsabili

Business Continuity Manager

Service Manager

APO09 - Manage Service Agreements

(Rating per ruolo :1.9)

Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.

Purpose

Ensure that IT services and service levels meet current and future enterprise needs.

Process Outcomes (Goals)
1. The enterprise can effectively utilise IT services as defined in a catalogue.
2. Service agreements reflect enterprise needs and the capabilities of IT.
3. IT services perform as stipulated in service agreements.

APO09.03 - Define and prepare service agreements. (Rating per ruolo :1.9)

Riferimenti alla Circ. BI 263

Cap.	**titolo**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	**from**
Customer requirements for quality management	**Business Executives (APO11.03)**

Output	**to**
SLAs	**Chief Executive Officer (APO05.03), Chief Information Officer (APO08.04), Chief Information Officer (DSS01.02), Chief Information Officer (DSS02.01), Head IT Operations (DSS02.02), Chief Operating Officer (DSS04.01), Chief Information Security Officer (DSS05.02), Chief Information Security Officer (DSS05.03)**
Operational level agreements (OLAs)	**Chief Information Officer (DSS01.02), Head IT Operations (DSS02.07), Business Continuity Manager (DSS04.03), Chief Information Security Officer (DSS05.03)**

Activities

Activity	Peso
B.1. Analyse requirements for new or changed service agreements received from business relationship management to ensure that the requirements can be matched. Consider aspects such as service times, availability, performance, capacity, security, continuity, compliance and regulatory issues, usability, and demand constraints.	**1.9**

Altri responsabili

Business Executives, Chief Information Officer, Head IT Operations, Head IT Administration

DSS02 - Manage Service Requests and Incidents

(Rating per ruolo :2.0)

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Purpose

Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

Process Outcomes (Goals)
1. IT-related services are available for use.
2. Incidents are resolved according to agreed-on service levels.
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.

DSS02.05 - Resolve and recover from incidents. (Rating per ruolo :2.0)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**

Inputs & Outputs

Input	from
Risk-related incident response plans	**Chief Information Officer (APO12.06)**
Known error records	**Head IT Operations (DSS03.03)**
Communication of knowledge learned	**Service Manager (DSS03.04)**

Output	to
Incident resolutions	**Service Manager (DSS03.04)**

Activities

Activity	Peso
B.1. Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).	**2.0**

Altri responsabili

Head Development, Head IT Operations, Information Security Manager

Business Continuity Manager

DSS04 - Manage Continuity

(Rating per ruolo :3.8)

Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

Purpose

Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

Process Outcomes (Goals)
1. Business-critical information is available to the business in line with minimum required service levels.
2. Sufficient resilience is in place for critical services.
3. Service continuity tests have verified the effectiveness of the plan.
4. An up-to-date continuity plan reflects current business requirements.
5. Internal and external parties have been trained in the continuity plan.

DSS04.03 - Develop and implement a business continuity response. (Rating per ruolo :3.6)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	**Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)**
9.I.4	**Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)**
9.A.I.1	**Premessa**
9.A.II.1	**Ambito del piano di continuità operativa**
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
OLAs	**Service Manager (APO09.03)**

Output	to
Incident response actions and communications	Chief Information Officer (DSS02.01)
BCP	(Internal)

Activities

Activity	Peso
B.1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.	2.8
B.2. Develop and maintain operational BCPs containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.	3.0
B.3. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.	2.8
B.4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.	2.5
B.5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.	2.8
B.6. Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.	2.5
B.7. Determine required skills for individuals involved in executing the plan and procedures.	2.5
B.8. Distribute the plans and supporting documentation securely to appropriately authorised interested parties and make sure they are accessible under all disaster scenarios.	2.6
S.1. Include information security requirements in the BCP.	1.8

Altri responsabili

Business Process Owners, Chief Information Officer, Head IT Operations

DSS04.04 - Exercise, test and review the BCP. (Rating per ruolo :3.3)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.I.3	Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)
9.I.4	Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)
9.A.I.1	Premessa
9.A.II.3	Definizione del piano di continuità operativa e gestione delle crisi
9.A.III.2	Definizione del piano di continuità operativa e gestione delle crisi

Inputs & Outputs

Output	to
Test objectives	**(Internal)**
Test exercises	**(Internal)**
Test results and recommendations	**(Internal)**

Activities

Activity	Peso
B.1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP in meeting business risk.	**2.6**
B.2. Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	**2.6**
B.3. Assign roles and responsibilities for performing continuity plan exercises and tests.	**2.4**
B.4. Schedule exercises and test activities as defined in the continuity plan.	**2.4**
B.5. Conduct a post-exercise debriefing and analysis to consider the achievement.	**2.5**
B.6. Develop recommendations for improving the current continuity plan based on the results of the review.	**2.4**

Altri responsabili

Business Process Owners, Audit, Chief Information Officer, Head IT Operations

DSS04.06 - Conduct continuity plan training. (Rating per ruolo :2.2)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.2	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Input	from
List of personnel requiring training	**(HR)**

Output	to
Training requirements	**Chief Information Officer (APO07.03)**
Monitoring results of skills and competencies	**Chief Information Officer (APO07.03)**

Activities

Activity	Peso
B.1. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.	**1.9**
B.2. Develop competencies based on practical training including participation in exercises and tests.	**1.6**
B.3. Monitor skills and competencies based on the exercise and test results.	**1.6**

Altri responsabili

Business Process Owners, Chief Information Officer, Head Development, Head IT Operations, Head IT Administration

DSS04.08 - Conduct post-resumption review. (Rating per ruolo :2.4)

Riferimenti alla Circ. BI 263

Cap.	titolo
9.A.II.3	**Definizione del piano di continuità operativa e gestione delle crisi**
9.A.III.3	**Comunicazioni alla Banca d'Italia**

Inputs & Outputs

Output	to
Post-resumption review report	**(Internal)**
Approved changes to the plans	**Business Executives (BAI06.01)**

Activities

Activity	Peso
B.1. Assess adherence to the documented BCP.	**1.8**
B.2. Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organisational structures and relationships.	**1.8**
B.3. Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.	**1.8**
B.4. Obtain management approval for any changes to the plan and apply via the enterprise change control process.	**1.8**

Altri responsabili

Business Process Owners, Chief Information Officer, Head IT Operations, Head IT Administration

C

D