Aegentra ACADEMY

Business Impact Analysis — ISO 22301:2019 Clause 8.2.2

Twelve activities with dependencies, MTPD, RTO, RPO and minimum service level

The BIA is the document everything else in a BCMS depends on, and the one an auditor opens first. The most common failure is assessing SYSTEMS instead of ACTIVITIES — a BIA that lists servers cannot produce a defensible recovery time objective. Worked for an APRA-regulated Australian financial services business, with the CPS 230 critical-operation flag included.

REF	BUSINESS ACTIVITY	OWNER	PRODUCTS/SERVICES SUPPORTED	KEY DEPENDENCIES	PEAK/CRITICAL TIMING	IMPACT AT 4H	IMPACT AT 24H	IMPACT AT 1 WEEK	MTPD	RTO	RPO	MINIMUM BUSINESS CONTINUITY OBJECTIVE	RECOVERY STRATEGY	CPS 230 CRITICAL OPERATION?
BIA-01	Customer payments processing	Head of Operations	All customer transactions	Core banking platform, payment gateway, SWIFT connection	Weekdays 09:00-17:00, month-end peak	Severe — customers cannot transact; regulator notification likely	Critical — media attention, APRA notification	Extreme — licence exposure	8 hours	4 hours	15 minutes	Process priority payments manually to a $50k daily cap	Active-passive across two regions; manual fallback documented and exercised half-yearly	Yes
BIA-02	Customer contact centre	Head of Customer	Complaints, hardship, general enquiries	Telephony platform, CRM, workforce scheduling	Weekdays 08:00-18:00	Moderate — queue times rise, complaints accumulate	Major — hardship obligations at risk	Severe — regulatory complaint exposure	24 hours	8 hours	4 hours	Divert to a reduced team handling hardship and complaints only	Cloud telephony with a second region; documented work-from-home fallback	Yes
BIA-03	Loan origination and approvals	Head of Lending	New lending	Origination platform, credit bureau feed, document store	Weekdays, quarter-end peak	Minor — applications queue	Moderate — settlement dates at risk, broker escalation	Major — measurable revenue loss and broker attrition	3 days	24 hours	4 hours	Manual assessment for applications already at settlement stage	Vendor SLA with a documented manual assessment process	Yes
BIA-04	Regulatory and statutory reporting	Chief Risk Officer	APRA and ASIC reporting	Data warehouse, reporting tool, source systems	Month-end and quarter-end only	Negligible outside reporting windows	Negligible outside windows	Severe if it spans a reporting deadline	5 days (1 day in a reporting window)	24 hours	24 hours	Compile the priority returns from source extracts manually	Extract snapshots retained; manual compilation procedure tested annually	Yes
BIA-05	Payroll	Head of People	**Staff payment**	Payroll platform, banking file transfer, HRIS	Fortnightly, two days before pay date	Negligible outside the pay cycle	Moderate near a pay date	Severe — staff unpaid, Fair Work exposure	5 days (12 hours near a pay date)	8 hours	24 hours	Repeat the prior period payment and reconcile afterwards	Payroll provider redundancy; prior-period repeat procedure documented	No
BIA-06	IT service desk	IT Manager	**Internal support for all activities**	Ticketing platform, remote access, telephony	Weekdays 08:00-18:00	Minor — staff self-serve	Moderate — incident backlog grows	Major — other activities begin to degrade	3 days	24 hours	8 hours	Email and phone intake with manual triage	Email fallback with a documented triage roster	No
BIA-07	Treasury and liquidity management	CFO	Funding and liquidity	Treasury platform, market data feeds, banking portals	Daily, morning cut-off critical	Critical — liquidity position unknown	Extreme — funding and covenant exposure	Extreme	4 hours	2 hours	15 minutes	Manage positions manually from broker confirmations	Secondary terminal at an alternate site; manual position workbook maintained daily	Yes

REF	BUSINESS ACTIVITY	OWNER	PRODUCTS/SERVICES SUPPORTED	KEY DEPENDENCIES	PEAK/CRITICAL TIMING	IMPACT AT 4H	IMPACT AT 24H	IMPACT AT 1 WEEK	MTPD	RTO	RPO	MINIMUM BUSINESS CONTINUITY OBJECTIVE	RECOVERY STRATEGY	CPS 230 CRITICAL OPERATION?
BIA-08	Fraud monitoring	Head of Financial Crime	Transaction monitoring and alerting	Monitoring platform, transaction feed, case management	Continuous, 24/7	Major — undetected fraud accumulates	Severe — customer loss and AUSTRAC exposure	Extreme	12 hours	4 hours	1 hour	Rule-based screening on high-value transactions only	Vendor redundancy plus a documented manual screening threshold	Yes
BIA-09	Customer onboarding and KYC	Head of Operations	**New customer acquisition**	Identity verification service, core platform, document capture	Weekdays	Minor	Moderate — acquisition stalls	Major — revenue and reputation	3 days	24 hours	4 hours	Manual identity verification for priority customers	Alternate identity provider contracted; manual procedure documented	No
BIA-10	Corporate email and collaboration	IT Manager	All activities	Microsoft 365, identity provider, network	Weekdays continuous	Moderate — coordination degrades	Major — most activities affected	Severe	24 hours	4 hours	1 hour	Mobile access and an out-of-band communication channel	Vendor SLA; out-of-band channel provisioned and tested half-yearly	Yes
BIA-11	Physical premises (head office)	Head of Facilities	**Staff working location**	Building access, power, network	Weekdays	Minor — staff work remotely	Minor — remote working absorbs it	Moderate — culture and supervision degrade	2 weeks	3 days	Not applicable	All staff work remotely; a small site for essential functions	Remote-first capability already proven; secondary site retained on standby	No
BIA-12	Data backup and restoration	IT Manager	Recovery of every other activity	Backup platform, immutable storage, restoration tooling	Continuous	Not customer-visible, but blocks all other recovery	Critical — recovery capability lost	Extreme	24 hours	8 hours	15 minutes	Restore from the most recent verified immutable copy	Immutable offsite copies; quarterly restore test with recorded actual times	Yes