

Kelompok 1

Mohamad Ikhsan Zulfadly 1202154138

Nyimas Marissa Gita Fitri 1202154354

Farhan Putra Riantono 1202150098

Faizal Sudrajat 1202150074

Farah Urfani Nugraha 1202152322

Anggit Nur Fitria 1202154362

Figure 22—Mapping COBIT 5 Enterprise Goals to IT-related Goals

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT-related Goal			Financial					Customer				Internal					Learning and Growth		
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S			S		S	P					
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Figure 22—Mapping COBIT 5 Enterprise Goals to IT-related Goals

		Enterprise Goal																
		Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT-related Goal		Financial					Customer					Internal					Learning and Growth	
Financial	01 Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03 Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04 Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05 Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06 Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07 Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09 IT agility	S	P	S			S		P			P		S	S		S	P
	10 Security of information, processing infrastructure and applications			P	P			P								P		
	11 Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12 Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14 Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15 IT compliance with internal policies			S	S											P		
Learning and Growth	16 Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17 Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Figure 23—Mapping COBIT 5 IT-related Goals to Processes

			IT-related Goal																																	
			Alignment of IT and business strategy		IT compliance and support for business compliance with external laws and regulations		Commitment of executive management for making IT-related decisions		Managed IT-related business risk		Realised benefits from IT-enabled investments and services portfolio		Transparency of IT costs, benefits and risk		Delivery of IT services in line with business requirements		Adequate use of applications, information and technology solutions		IT agility		Security of information, processing infrastructure and applications		Optimisation of IT assets, resources and capabilities		Enablement and support of business processes by integrating applications and technology into business processes		Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards		Availability of reliable and useful information for decision making		IT compliance with internal policies		Competent and motivated business and IT personnel		Knowledge, expertise and initiatives for business innovation	
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17																	
COBIT 5 Process			Financial						Customer			Internal						Learning and Growth																		
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S	S																
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P																	
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S																	
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S																	
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S																	
Align, Plan and Organise	AP001	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P																	
	AP002	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P																	
	AP003	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S																	
	AP004	Manage Innovation	S			S	P			P	P		P	S		S			P																	
	AP005	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S																	
	AP006	Manage Budget and Costs	S		S	S	P	P	S	S			S		S																					
	AP007	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P																	
	AP008	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P																	
	AP009	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S																			
	AP010	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S																	
	AP011	Manage Quality	S	S		S	P		P	S	S	S		S		P	S	S	S	S																
	AP012	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S	S																
	AP013	Manage Security		P		P		P	S	S		P				P																				

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities		
Risk Scenario		COBIT 5 Process Capabilities
<i>If the scenario is relevant and inherently likely...</i>	<i>...given these negative examples...</i>	<i>...then consider whether these COBIT 5 processes need improvement. Note: In this column, next to each process number is an example from the process to consider. These are not the process names.</i>
Benefit/value enablement risk		
IT programme selection	<ul style="list-style-type: none"> Incorrect programmes selected for implementation and misaligned with corporate strategy and priorities Duplication among different initiatives New and important programme creates long-term incompatibility with the enterprise architecture 	<ul style="list-style-type: none"> AP002 Aligned business and IT strategy AP003 Compatibilities with enterprise architecture AP004 Identification of innovation opportunities AP005 Portfolio management decisions BAI01 Programme management planning and co-ordination
New technologies	<ul style="list-style-type: none"> Failure to adopt and exploit new technologies (i.e., functionality, optimisation) in a timely manner New and important technology trends not identified Inability to use technology to realise desired outcomes (e.g., failure to make required business model or organisational changes) 	<ul style="list-style-type: none"> EDM04 Resource management direction and/or oversight AP002 Strategy identifying technology opportunities AP003 Enterprise architecture aligned with current technology trends AP004 New and important technology trends identified BAI02 Ability to use new technology to define new business models BAI03 Adoption and exploitation of new technologies
Technology selection	<ul style="list-style-type: none"> Incorrect technologies (i.e., cost, performance, features, compatibility) selected for implementation 	<ul style="list-style-type: none"> AP002 Effective strategic technology selection AP003 Enterprise architecture technology consistency BAI03 Identifying and building solutions AP013 Security impacts of technology selection
IT investment decision making	<ul style="list-style-type: none"> Business managers or representatives not involved in important IT investment decision making regarding new applications, prioritisation or new technology opportunities 	<ul style="list-style-type: none"> EDM02 Value management direction and/or oversight AP002 Business involvement in IT strategic planning AP003 Investment fit with target enterprise architecture AP005 Portfolio management decisions AP006 Investment monitoring AP008 Understanding of business expectations and opportunities to leverage IT BAI01 Programme management stage-gating
Accountability over IT	<ul style="list-style-type: none"> Business not assuming accountability over those IT areas it should such as functional requirements, development priorities and assessing opportunities through new technologies 	<ul style="list-style-type: none"> EDM01-05 Executive management accountability for IT-related decisions AP001 Business and IT-related roles and responsibilities AP009 Clear and approved service agreements AP010 Defined and managed supplier agreements and relationships BAI05 Enabling organisational changes with respect to IT accountability and GEIT
IT project termination	<ul style="list-style-type: none"> Projects that are failing due to cost, delays, scope creep or changed business priorities not terminated in a timely manner 	<ul style="list-style-type: none"> EDM01 GEIT policies, organisation structures and roles EDM02 Value governance monitoring EDM04 Resource governance monitoring BAI01 Programme/project management stage-gating AP005 Effective portfolio management decision making AP006 Investment monitoring MEA01 Performance monitoring
IT project economics	<ul style="list-style-type: none"> Isolated IT project budget overrun Consistent and important IT projects budget overruns Absence of view on portfolio and project economics 	<ul style="list-style-type: none"> EDM01 GEIT policies, organisation structures and roles EDM02 Value governance monitoring EDM04 Resource governance monitoring AP006 Investment monitoring BAI01 Programme/project management planning and monitoring

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities (cont.)

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities (cont.)		
Risk Scenario		COBIT 5 Process Capabilities
<i>If the scenario is relevant and inherently likely...</i>	<i>...given these negative examples...</i>	<i>...then consider whether these COBIT 5 processes need improvement. Note: In this column, next to each process number is an example from the process to consider. These are not the process names.</i>
Programme/project delivery risk		
Architectural agility and flexibility	<ul style="list-style-type: none"> Complex and inflexible IT architecture obstructing further evolution and expansion 	<ul style="list-style-type: none"> AP001 Efficient and defined business and IT-related processes EDM04 Governance over resource optimisation AP002 Responsive strategic planning AP003 Maintenance of enterprise architecture AP004 Innovation and initiation of change AP005 Portfolio management decision taking BAI02_03 Agile development life cycle methods AP013 Maintaining security in an agile and flexible environment
Integration of IT within business processes	<ul style="list-style-type: none"> Extensive dependency and use of end-user computing and <i>ad hoc</i> solutions for important information needs Separate and non-integrated IT solutions to support business processes 	<ul style="list-style-type: none"> EDM01 GEIT policies, organisation structures and roles AP001 Business and IT-related roles and responsibilities AP002 Alignment of business and IT strategies AP003 Architectural designs and decisions AP008 Business and IT relations BAI02 Definition and understanding of business requirements BAI03 Adaptation of business processes to new IT solutions BAI05 Managing organisational changes with regards to IT
Software implementation	<ul style="list-style-type: none"> Operational glitches when new software is made operational Users not prepared to use and exploit new application software 	<ul style="list-style-type: none"> AP011 Consistent and effective quality management activities BAI01 Project management BAI02 Requirements definitions BAI03 Solution development BAI05 Managing organisational changes with regards to software implementation BAI06 Change management BAI07 Extensive solution testing BAI08 Knowledge support
Project delivery	<ul style="list-style-type: none"> Occasional late IT project delivery by internal development department Routinely important delays in IT project delivery Excessive delays in outsourced IT development project 	<ul style="list-style-type: none"> EDM01 GEIT policies, organisation structures and roles EDM02 Value governance monitoring AP006 Investment monitoring BAI01 Programme/project management planning and monitoring
Project quality	<ul style="list-style-type: none"> Insufficient quality of project deliverables due to software, documentation or compliance with functional requirements 	<ul style="list-style-type: none"> AP003 Architecture standards AP011 Consistent and effective quality management activities BAI01 Programme/project quality management planning and monitoring
Service delivery/IT operations risk		
State of infrastructure technology	<ul style="list-style-type: none"> Obsolete IT technology cannot satisfy new business requirements such as networking, security and storage 	<ul style="list-style-type: none"> EDM04 Resource management direction and/or oversight AP002 Recognising and strategically addressing current IT capability issues AP003 Maintaining enterprise architecture AP004 Identifying important technology trends BAI03 Maintaining infrastructure BAI04 Planning for and addressing capacity and performance issues BAI09 Maintaining assets
Ageing of application software	<ul style="list-style-type: none"> Application software that is old, poorly documented, expensive to maintain, difficult to extend or not integrated in current architecture 	<ul style="list-style-type: none"> EDM04 Resource management direction and/or oversight AP002 Recognising and strategically addressing current IT capability issues AP003 Maintaining enterprise architecture AP004 Identifying new and important technology trends BAI03 Maintaining applications BAI09 Maintaining assets DSS06 Business process controls

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities (cont.)

Risk Scenario		COBIT 5 Process Capabilities
<i>If the scenario is relevant and inherently likely...</i>	<i>...given these negative examples...</i>	<i>...then consider whether these COBIT 5 processes need improvement. Note: In this column, next to each process number is an example from the process to consider. These are not the process names.</i>
Service delivery/IT operations risk (cont.)		
Regulatory compliance	<ul style="list-style-type: none"> Non-compliance with regulations of accounting or manufacturing 	<ul style="list-style-type: none"> EDM01 GEIT compliance policies and roles APO01 Policies and guidance on regulatory compliance APO02 Planning for regulatory requirements BAI02 Identifying and defining regulatory requirements MEA03 Monitoring compliance requirements and current status
Selection/performance of third-party suppliers	<ul style="list-style-type: none"> Inadequate support and services delivered by vendors, not in line with SLAs Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement 	<ul style="list-style-type: none"> APO10 Effective supplier selection, management and relationships BAI03 Effective management of procurements
Infrastructure theft	<ul style="list-style-type: none"> Theft of laptop with sensitive data Theft of a substantial number of development servers 	<ul style="list-style-type: none"> APO01 Policies and guidance on protection of assets APO07 References and background checks on new hires and contractors BAI03 Protection of critical assets during maintenance activities DSS05 Physical security measures
Destruction of infrastructure	<ul style="list-style-type: none"> Destruction of data centre due to sabotage or other causes Accidental destruction of individual laptops 	<ul style="list-style-type: none"> DSS01 Environmental protection and facilities management DSS05 Physical security measures
IT staff	<ul style="list-style-type: none"> Departure or extended unavailability of key IT staff Key development team leaving the enterprise Inability to recruit IT staff 	<ul style="list-style-type: none"> APO07 Development and retention of IT staff resources BAI08 Managing tacit knowledge
IT expertise and skills	<ul style="list-style-type: none"> Lack or mismatch of IT-related skills within IT due to new technologies or other causes Lack of business understanding by IT staff 	<ul style="list-style-type: none"> APO07 Definition and development of business and IT staff competency requirements BAI08 Knowledge support
Software integrity	<ul style="list-style-type: none"> Intentional modification of software leading to wrong data or fraudulent actions Unintentional modification of software leading to unexpected results Unintentional configuration and change management errors 	<ul style="list-style-type: none"> BAI02 Definition of application control requirements BAI06 Change management BAI07 Testing and acceptance practices BAI10 Configuration data DSS05 Access controls DSS06 Business process controls
Infrastructure (hardware)	<ul style="list-style-type: none"> Misconfiguration of hardware components Damage of critical servers in the computer room due to accident or other causes Intentional tampering with hardware such as security devices 	<ul style="list-style-type: none"> BAI03 Protection of critical assets during maintenance activities BAI10 Configuration data DSS05 Physical security measures
Software performance	<ul style="list-style-type: none"> Regular software malfunctioning of critical application software Intermittent performance problems with important system software 	<ul style="list-style-type: none"> BAI03 Software development quality assurance BAI04 Planning for and addressing capacity and performance issues DSS03 Root cause analysis and problem resolution
System capacity	<ul style="list-style-type: none"> Inability of systems to handle transaction volumes when user volumes increase Inability of systems to handle system load when new applications or initiatives are deployed 	<ul style="list-style-type: none"> APO03 Architecture principles for scalability and agility BAI03 Maintaining infrastructure BAI04 Planning for and addressing capacity and performance issues
Ageing of infrastructural software	<ul style="list-style-type: none"> Use of unsupported versions of operating system software Use of old database system 	<ul style="list-style-type: none"> EDM04 Resource management direction and/or oversight APO02 Recognising and strategically addressing current IT capability issues APO03 Maintaining enterprise architecture APO04 Identifying new and important technology trends BAI03 Maintaining infrastructure DSS08 Problems relating to business process controls
Malware	<ul style="list-style-type: none"> Intrusion of malware on critical operational servers Regular infection of laptops with malware 	<ul style="list-style-type: none"> APO01 Policies and guidance on use of software DSS05 Malicious software detection

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities (cont.)

Risk Scenario		COBIT 5 Process Capabilities
<i>If the scenario is relevant and inherently likely...</i>	<i>...given these negative examples...</i>	<i>...then consider whether these COBIT 5 processes need improvement. Note: In this column, next to each process number is an example from the process to consider. These are not the process names.</i>
Service delivery/IT operations risk (cont.)		
Logical attacks	<ul style="list-style-type: none"> • Virus attack • Unauthorised users trying to break into systems • Denial-of-service attack • Web site defacing • Industrial espionage 	<ul style="list-style-type: none"> • AP001 Policies and guidance on protection and use of IT assets • BAI03 Security requirements in solutions • DSS05 Access controls and security monitoring
Information media	<ul style="list-style-type: none"> • Loss/disclosure of portable media (e.g., CD, universal serial bus [USB] drives, portable disks) containing sensitive data • Loss of backup media • Accidental disclosure of sensitive information due to failure to follow information handling guidelines 	<ul style="list-style-type: none"> • AP001 Policies and guidance on protection and use of IT assets • DSS05, 06 Protection of mobile and/or removable storage and media devices
Utilities performance	<ul style="list-style-type: none"> • Intermittent utilities (e.g., telecom, electricity) failure • Regular, extended utilities failures 	<ul style="list-style-type: none"> • AP008 Relationships/management of key utility suppliers • DSS01 Environmental protection and facilities management
Industrial action	<ul style="list-style-type: none"> • Inaccessible facilities and building due to labour union strike • Unavailable key staff due to industrial action 	<ul style="list-style-type: none"> • AP007 Staff relationships and key individuals • BAI08 Managing staff knowledge
Data(base) integrity	<ul style="list-style-type: none"> • Intentional modification of data (e.g., accounting, security-related data, sales figures) • Database (e.g., client or transactions database) corruption 	<ul style="list-style-type: none"> • AP003 Information architecture and data classification • BAI03 Development standards • BAI06 Change management • DSS01 Managing data storage • DSS05 Access controls
Logical trespassing	<ul style="list-style-type: none"> • Users circumventing logical access rights • Users obtaining access to unauthorised information • Users stealing sensitive data 	<ul style="list-style-type: none"> • AP001 Policies and guidance on protection and use of IT assets • DSS05 Access controls and security monitoring • AP007 Contract staff policies
Operational IT errors	<ul style="list-style-type: none"> • Operator errors during backup, upgrades of systems or maintenance of systems • Incorrect information input 	<ul style="list-style-type: none"> • AP007 Staff training • DSS01 Operations procedures • DSS06 Business process controls
Contractual compliance	<ul style="list-style-type: none"> • Non-compliance with software licence agreements (e.g., use and/or distribution of unlicensed software) • Contractual obligations as service provider with customers/clients not met 	<ul style="list-style-type: none"> • AP009 Monitoring service agreements • AP010 Supplier agreements and relationship monitoring • DSS02 Software licence management • MEA03 Contractual compliance requirements and current status monitoring
Environmental	<ul style="list-style-type: none"> • Use of equipment that is not environmentally friendly (e.g., high level of power consumption, packaging) 	<ul style="list-style-type: none"> • AP003 Incorporation of environmentally friendly principles in enterprise architecture • BAI03 Selection of solutions and procurement policies • DSS01 Environmental and facilities management
Acts of nature	<ul style="list-style-type: none"> • Earthquake • Tsunami • Major storm/hurricane • Major wildfire 	<ul style="list-style-type: none"> • DSS01 Environmental and facilities management • DSS05 Physical security • DSS04 Manage continuity

Cobit 5 Process Probabilities

- IT Staff :
 - APO07 Development and retention of it staff resources
- Technology Selection:
 - BAI03 Identifying and building solution
- Ageing of application software
 - APO04 Identifying new & important technology trends
- IT Expertise
 - APO07 Definition and development of business and IT staff competency requirements
- Database integrity DSS01 Managing data storage