

ABSTRAK

Pada saat ini audit sistem informasi sangat diperlukan karena perkembangan teknologi informasi yang semakin maju dan menjadi unsur penting dalam suatu organisasi. Salah satu framework yang sering digunakan untuk melakukan proses audit ini adalah COBIT 5, COBIT 5 dipilih karena dapat meningkatkan keamanan sistem informasi yang sedang dijalankan dan dapat menjadi alat bantu yang dapat memecahkan permasalahan dalam teknologi informasi. Metode penelitian yang digunakan pada audit ini ialah dengan observasi dan wawancara. Dikarenakan pembahasan ini menyangkut informasi yang sensitif, maka atas permintaan pihak bank, nama bank dirubah menjadi Bank XYZ. PT. Bank XYZ merupakan salah satu organisasi yang bergerak dalam melayani penyimpanan uang dan sudah menerapkan sistem informasi secara *online* untuk setiap transaksi perbankan yang terjadi. Salah satu aspek penting dalam sistem informasi adalah keamanan yang baik, untuk menangani celah dan menentukan tingkat keamanan pada keamanan sistem informasi agar menunjang perkembangan dari PT. Bank XYZ. Dengan adanya audit sistem informasi ini, PT. Bank XYZ akan dapat mengenali kelemahan yang terdapat pada sistem, dan menangani masalah yang terjadi dan juga dapat melakukan peningkatan keamanan pada sistem informasi yang sudah ada.

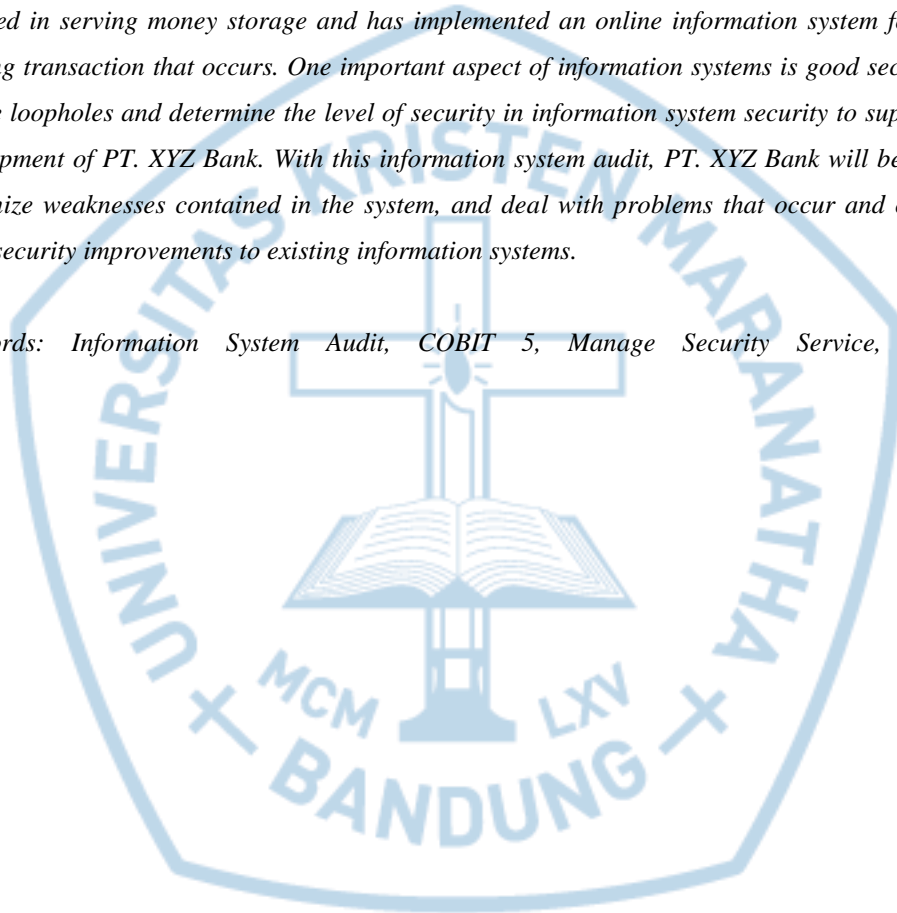
Kata kunci: Audit Sistem Informasi, COBIT 5, Manage Security Service, DSS05.



ABSTRACT

At this time the information system audit is very necessary because the development of information technology is increasingly advanced and an important element in an organization. One framework that is often used to carry out this audit process is COBIT 5, COBIT 5 chosen because it can improve the security of information systems that are being run and can be a tool that can solve problems in information technology. The research method used in this audit is by observation and interview. Because this discussion concerns sensitive information, at the request of the bank, the bank's name is changed to Bank XYZ. PT. Bank XYZ is one of the organizations engaged in serving money storage and has implemented an online information system for every banking transaction that occurs. One important aspect of information systems is good security, to handle loopholes and determine the level of security in information system security to support the development of PT. XYZ Bank. With this information system audit, PT. XYZ Bank will be able to recognize weaknesses contained in the system, and deal with problems that occur and can also make security improvements to existing information systems.

Keywords: Information System Audit, COBIT 5, Manage Security Service, DSS05.



DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN.....	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA.....	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xiv
DAFTAR SINGKATAN	xvi
DAFTAR ISTILAH	xvii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup.....	2
1.5 Sumber Data.....	2
1.6 Sistematika Penyajian	3
BAB 2 KAJIAN TEORI	4
2.1 Pengertian Sistem Informasi	4
2.2 Pengertian Audit Sistem Informasi	4
2.3 Tahapan Audit Sistem Informasi	5
2.4 COBIT 5.....	6
2.4.1 Prinsip-Prinsip COBIT 5.....	7

2.4.2 Domain dan Proses pada COBIT 5	9
2.4.3 Diagram RACI	10
2.4.4 Work Product	11
2.4.5 Capability Level	11
2.4.6 <i>Rating Scale</i>	13
2.4.7 SLA	14
2.4.8 OLA	14
2.5 <i>Deliver, Service, And Support 05 (DSS05)</i>	14
2.5.1 DSS05.01 <i>Protect Agains Malware</i>	15
2.5.2 DSS05.02 <i>Manage Network and Connectivity Security</i>	15
2.5.3 DSS05.03 <i>Manage Endpoint Security</i>	15
2.5.4 DSS05.04 <i>Manage User Identify and Logical Access</i>	15
2.5.5 DSS05.05 <i>Manage Physical Access to IT Access</i>	15
2.5.6 DSS05.06 <i>Manage Sensitive Document and Output Device</i>	16
2.5.7 DSS05.07 <i>Monitor the Infrastructure for Security Related Event</i>	16
2.6 Audit Program	17
BAB 3 ANALISIS DAN HASIL PENELITIAN	20
3.1 PT Bank XYZ	20
3.1.1 Profil Organisasi	20
3.1.2 Profil Divisi TI di Bank XYZ	21
3.1.3 Visi dan Misi	22
3.2 Audit Program	23
3.2.1 Phase A - Menentukan <i>Plan Assesment/Assurance Initiative</i>	23
3.2.1.1 <i>Determine The Stakeholder of The Assurance</i>	23
3.2.1.2 <i>Determine The Assurance Objectives Based on Assesment of the External and Internal Context</i>	25

3.2.1.2.1	<i>Understand The Enterprise Strategy and Priorities</i>	25
3.2.1.2.2	<i>Understand The Internal Context of The Enterprise</i>	26
3.2.1.2.3	<i>Understand the External Context of the Enterprise</i>	26
3.2.1.2.4	<i>Identified Strategic Priorities into concrete objectives for the Assurance Engagement</i>	27
3.2.1.2.5	<i>Define The Organizational Boundaries of the Assurance Initiative</i>	27
3.2.1.3	<i>Determine the Enablers In Scope and the Instance of the Enablers in Scope</i>	27
3.2.1.3.1	<i>Define the Process in Scope Review</i>	28
3.2.1.3.2	<i>Define the Related Enablers</i>	28
3.2.1.3.2.1	<i>Principles, Policies and Frameworks</i>	28
3.2.1.3.2.2	<i>Organisational Structures</i>	31
3.2.1.3.2.3	<i>Culture, Ethics and Behaviour</i>	32
3.2.1.3.2.4	<i>Information Item</i>	32
3.2.1.3.2.5	<i>Service, Infrastructure and Application</i>	34
3.2.1.3.2.6	<i>People, Skill and Competencies</i>	35
3.2.2	<i>Phase B – Memahami enabler, set Kriteria dan performa Assesment.</i>	39
3.2.2.1	<i>Enterprise Goals dan IT-Related Goals</i>	39
3.2.2.1.1	<i>Assess Enterprise Goals</i>	39
3.2.2.1.2	<i>Assess IT-Related Goals</i>	40
3.2.2.2	<i>Obtain Understanding of The Process in Scope and set Suitable Assessment Criteria</i>	41
3.2.2.2.1	<i>Understand The Process Purpose</i>	42
3.2.2.2.2	<i>Assess Process Goals</i>	42
3.2.2.2.2.1	<i>DSS05.01 Protect Against Malware</i>	42
3.2.2.2.2.2	<i>DSS05.02 Manage Network and Connectivity Security</i>	43

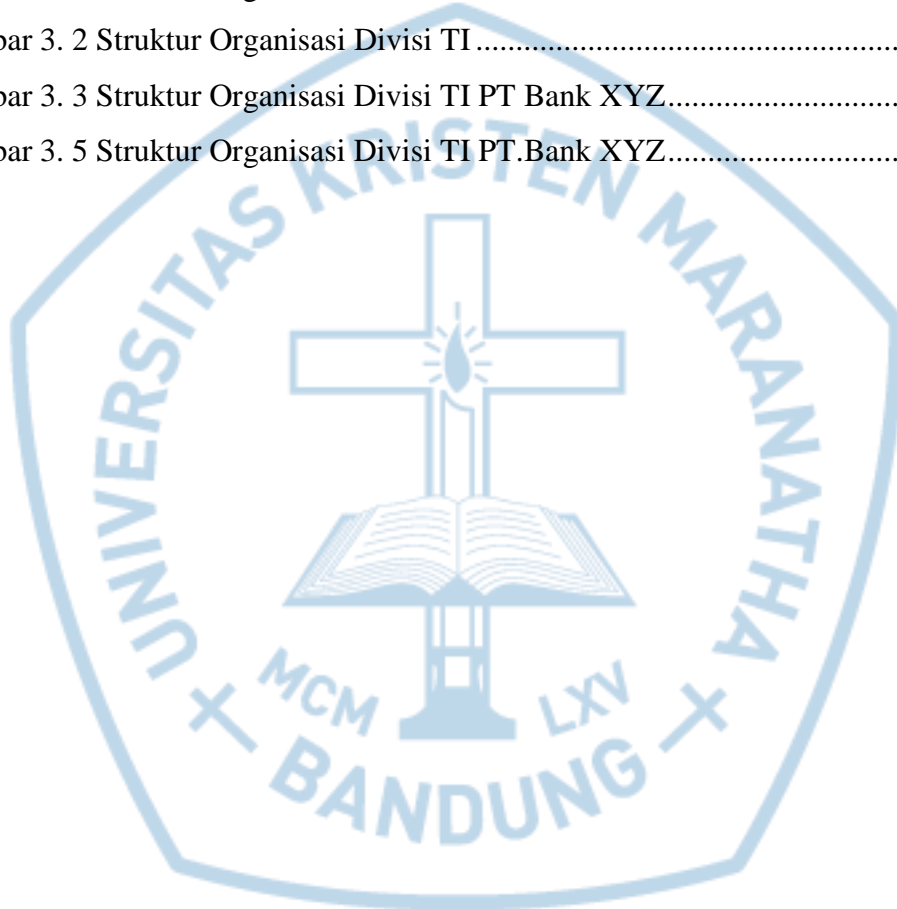
3.2.2.2.2.3 DSS05.03 <i>Manage Endpoint Security</i>	45
3.2.2.2.2.4 DSS05.04 <i>Manage User Identify and Logical Access</i>	46
3.2.2.2.2.5 DSS05.05 <i>Manage Physical Access to IT Assets</i>	48
3.2.2.2.2.6 <i>DSS05.06 Manage Sensitive Documents adn Output Devices</i>	50
3.2.2.2.2.7 DSS05.07 <i>Monitor The Infrastructure for Security-Related Events</i>	51
3.2.2.2.3 <i>Work Product</i>	52
3.2.2.2.3.1 <i>Work Product DSS05.01</i>	53
3.2.2.2.3.2 <i>Work Product DSS05.02</i>	53
3.2.2.2.3.3 <i>Work Product DSS05.03</i>	54
3.2.2.2.3.4 <i>Work Product DSS05.04</i>	54
3.2.2.2.3.5 <i>Work Product DSS05.05</i>	55
3.2.2.2.3.6 <i>Work Product DSS05.06</i>	55
3.2.2.2.3.7 <i>Work Product DSS05.07</i>	56
3.2.2.2.4 <i>RACI CHART</i>	57
3.2.2.2.5 <i>Capability Level</i>	58
3.2.2.3 <i>Understand and Assess The Principle, Policies and Framework</i> .	71
3.2.2.3.1 <i>Understand the Principle, Policies and Framework</i>	71
3.2.2.3.2 <i>Understand The Stakeholder Principle, Policies and Framework</i>	74
3.2.2.3.3 <i>Understand The Goals for the Principle, Policies and Framework</i>	74
3.2.2.3.4 <i>Understand Good Practices related to the Principles, Policies and Framework</i>	75
3.2.2.4 <i>Understand and Assess The Organisational Structures</i>	76
3.2.2.4.1 <i>Understand The Organisational Structure Context</i>	76

3.2.2.4.2	<i>Understand all Stakeholders of the Organisational Structure/Function.</i>	76
3.2.2.4.3	<i>Understand The Goals of The Organisational Structure</i>	82
3.2.2.4.4	<i>Good Practices for the Organisational Structure against which it will be assessed</i>	87
3.2.2.4.5	<i>Understand The Organisational Structure Life Cycle is Managed</i>	89
3.2.2.5	<i>Understand and Assess Culture, Ethics and Behaviour.</i>	89
3.2.2.5.1	<i>Understand The Culture, Ethics and Behaviour context.</i>	89
3.2.2.5.2	<i>Understand The Major Stakeholders of The Culture, Ethics and Behaviour.</i>	90
3.2.2.5.3	<i>Understand The Goals for The Culture, Ethics and Behaviour.</i>	90
3.2.2.5.4	<i>Understand The Life Cycle stages of the Culture Culture, Ethics and Behaviour</i>	91
3.2.2.5.5	<i>Understand Good Practices When Dealing with Culture, Ethics and Behaviour</i>	91
3.2.2.6	<i>Understand and Assess Information Items.</i>	92
3.2.2.6.1	<i>Understand The Information Item Context.</i>	92
3.2.2.6.2	<i>Understand The Major Stakeholders of The Information Item.</i>	93
3.2.2.6.3	<i>Understand The Major Quality Criteria for the Information Item.</i>	94
3.2.2.6.4	<i>Understand The Life Cycle Stages of The Information Item.</i>	96
3.2.2.6.5	<i>Understand Important Attributes of The Information Item and Expected Values.</i>	97
3.2.2.7	<i>Understand and Assess of The Services, Infrastructure and Applications</i>	98

3.2.2.7.1 <i>Understand The Services, Infrastructure and Applications Context</i>	98
3.2.2.7.2 <i>Understand The Major stakeholders of The Services, Infrastructure and Applications context</i>	99
3.2.2.7.3 <i>Understand The Major Goals for The Services, Infrastructure and Applications.</i>	99
3.2.2.7.4 <i>Understand The life cycle stages of the Services, Infrastructure and Applications</i>	100
3.2.2.7.5 <i>Understand Good Practices related to the Services, Infrastructure and Application</i>	101
3.2.2.8 <i>Understand and Assess People, Skill and Competencies</i>	101
3.2.2.8.1 <i>Understand The People, Skill and Competencies Context.</i> ...	101
3.2.2.8.2 <i>Understand The Major stakeholders for People, Skills and Competencies.</i>	104
3.2.2.8.3 <i>Understand The Major Goals for The People, Skills and Competencies.</i>	104
3.2.2.8.4 <i>Understand The Life Cycle Stages of The People, Skills and Competencies.</i>	105
3.2.2.8.5 <i>Understand Good Practice Related to The People, Skills and Competencies and Expected Values</i>	106
BAB 4 SIMPULAN DAN SARAN	108
4.1 Simpulan	108
4.2 Saran	108
DAFTAR PUSTAKA	110

DAFTAR GAMBAR

Gambar 2. 1 COBIT 5 Principles.....	7
Gambar 2. 2 Domain dan Proses COBIT 5 (Sumber : ISACA,2012).....	9
Gambar 2. 3 Diagram RACI DSS05 (Sumber : ISACA,2012).....	10
Gambar 2. 4 Process Capability level	12
Gambar 2. 5 Audit Program	17
Gambar 3. 1 Struktur Organisasi PT BANK XYZ	21
Gambar 3. 2 Struktur Organisasi Divisi TI	22
Gambar 3. 3 Struktur Organisasi Divisi TI PT Bank XYZ.....	31
Gambar 3. 5 Struktur Organisasi Divisi TI PT.Bank XYZ.....	76



DAFTAR TABEL

Tabel 2. 1 Kriteria Kerja COBIT	6
Tabel 2. 2 Work Product	11
Tabel 2. 3 Rating Scale	13
Tabel 3. 8 Enterprise Goals	39
Tabel 3. 9 <i>IT-Related Goals</i>	40
Tabel 3. 1 Hasil Analisis Pada Proses DSS05.01	42
Tabel 3. 2 Hasil Analisis Pada Proses DSS05.02	44
Tabel 3. 3 Hasil Analisis Pada Proses DSS05.03	45
Tabel 3. 4 Hasil Analisis Pada Proses DSS05.04	46
Tabel 3. 5 Hasil Analisis Pada Proses DSS05.05	48
Tabel 3. 6 Hasil Analisis Pada Proses DSS05.06	50
Tabel 3. 7 Hasil Analisis Pada Proses DSS05.07	51
Tabel 3. 11 Work Product DSS05.01	53
Tabel 3. 12 Work Product DSS05.02	53
Tabel 3. 13 Work Product DSS05.03	54
Tabel 3. 14 Work Product DSS05.04	55
Tabel 3. 15 Work Product DSS05.05	55
Tabel 3. 16 <i>Work Product</i> DSS05.06	56
Tabel 3. 17 <i>Work Product</i> DSS05.07	56
Tabel 3. 10 Perbandingan RACI Charts Proses DSS05 antara COBIT 5 Pada PT. Bank XYZ	57
Tabel 3. 18 Hasil Penilaian Capality Level DSS05 Pada PT. Bank XYZ	58
Tabel 3. 19 Work Product	68
Tabel 3. 20 Hasil Penilaian keefektifan prinsip, kebijakan dan kerangka kerja ...	74
Tabel 3. 21 Hasil Penilaian praktek yang baik pada prinsip, kebijakan dan kerangka kerja	75
Tabel 3. 22 Hasil Penilaian praktek yang baik pada struktur organisasi	88
Tabel 3. 23 Hasil Penilaian elemen siklus hidup pada organisasi	89
Tabel 3. 24 Hasil Penilaian tujuan, budaya dan perilaku	91
Tabel 3. 25 Hasil Penilaian praktik yang baik pada budaya, etika dan perilaku ...	91
Tabel 3. 26 Hasil Penilaian stakholder item informasi	93

Tabel 3. 27 Hasil Penilaian kriteria kualitas utama item informasi	94
Tabel 3. 28 Hasil Penilaian siklus hidup item informasi	96
Tabel 3. 29 Hasil Penilaian desain item informasi.....	97
Tabel 3. 30 Hasil Penilaian tujuan layananan, infrastruktur dan aplikasi	99
Tabel 3. 31 Hasil Penilaian praktek yang baik pada layanan, infrastruktur dan aplikasi	101
Tabel 3. 32 Hasil Penilaian kriteria keterampilan dan kompetensi.....	101
Tabel 3. 33 Hasil Penilaian Tujuan keterampilan dan kompetensi.....	104
Tabel 3. 34 Hasil Penilaian siklus hidup orang, keterampilan dan kompetensi..	105
Tabel 3. 35 Hasil Penilaian praktik yang baik pada orang, keterampilan dan kompetensi	106



DAFTAR SINGKATAN

TI	Teknologi Informasi
DSS	<i>Delivery Support System</i>
SLA	<i>Service Level Agreement</i>
OLA	<i>Operational Level Agreement</i>
KPI	<i>Key Performance Indicator</i>
DC	<i>Data Center</i>
CASA	<i>Current Account Saving Account</i>
UAT	<i>User Acceptance Test</i>
SIT	<i>Sytem Integration Test</i>
RSTI	Rencana Strategis Teknologi Informasi
ATM	<i>Automated Teller Machine</i>
COBIT	<i>Control Objective for Information and Related Technologies</i>
QA	<i>Quality Assurance Management</i>
SPG	<i>Strategic, Planning & Governance</i>
SNM	<i>System & Network Management</i>
CBA	<i>Core Banking Application</i>
HOA	<i>Head Office Application</i>
LPM	<i>Liaison & Project Management</i>
SI	<i>Switching & Interchange</i>
DCO	<i>Helpdesk & Data Center Operation</i>
DWH	<i>Data Warehouse Development</i>
ITRSM	<i>IT Risk & Security Management</i> <i>Divisi HC Divisi Human Capital</i>
CIF	<i>Customer Information File</i>

DAFTAR ISTILAH

Audit	proses pengumpulan data dan pengevaluasian bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah diterapkan dan menerapkan sistem pengendalian internal yang memadai, semua aktiva dilindungi dengan baik atau disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer
Audit Sistem Informasi	proses pengumpulan data dan pengevaluasian bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah diterapkan dan menerapkan sistem pengendalian internal yang memadai, semua aktiva dilindungi dengan baik atau disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer
<i>Network Monitoring</i>	<i>Network monitoring</i> menyediakan pemantauan secara terus menerus dan real time terhadap setiap komponen jaringan dan memberikan notifikasi pada <i>network administrator</i> .
<i>Data Recovery</i>	Pemulihan terhadap data yang hilang atau rusak, yang dapat dilakukan secara tepat waktu jika terjadi insiden keamanan, yang didefinisikan dalam bentuk <i>recovery point objective</i> dan <i>recovery time objective</i> .
<i>Fee Based</i>	Keuntungan yang didapat dari transaksi yang diberikan dalam jasa-jasa bank lainnya.
<i>Operating System</i>	Lapisan yang menghubungkan perangkat keras dengan perangkat lunak sistem informasi.
<i>Internet Banking</i>	Layanan berbasis web yang memungkinkan nasabah untuk melakukan transaksi bank melalui berbagai browser internet yang mengakomodir kebutuhan personal, korporat, trading, hingga fungsi portal untuk pendukung penyaluran DPLK.
<i>SMS Banking</i>	Aplikasi yang memungkinkan nasabah mendapatkan layanan perbankan seperti melakukan transaksi dan mendapat notifikasi melalui <i>Short Messaging Service</i> .
<i>M-Banking</i>	Aplikasi seluler yang memungkinkan nasabah melakukan transaksi dan layanan perbankan melalui mobile-based solutions, termasuk <i>mobile applications</i> dan USSD.
<i>Security Awareness</i>	Kesadaran terhadap keamanan informasi (<i>security awareness</i>) kepada karyawan dilakukan dengan cara memberikan pengetahuan tentang perilaku keamanan yang baik dan penting untuk dijalankan untuk meningkatkan proteksi dan pengamanan terhadap aset-aset IT.
<i>Network Security</i>	Perlindungan keamanan di setiap komponen jaringan perusahaan yang digunakan sebagai jalur lalu lintas data