

ABSTRAK

Teknologi Informasi (TI) saat ini menjadi bagian yang tidak terpisahkan dan terintegrasi dengan tujuan bisnis suatu organisasi. Dengan bantuan TI, proses bisnis yang terjadi di dalam organisasi dapat dilakukan dengan cepat dan efisien. Selain memudahkan perusahaan, teknologi informasi tidak luput dari berbagai ancaman secara fisik maupun non fisik. Untuk mencegah berbagai ancaman tersebut perusahaan perlu melakukan analisis dan evaluasi secara berkala. Dalam laporan ini diambil kasus yaitu Bank QNB Kesawan. Teori yang digunakan yaitu COBIT 4.1 domain *Deliver and Support* (DS) 5 *Ensure System Security*. Domain DS 5 ini membahas tentang kebutuhan untuk mempertahankan integritas informasi serta melindungi aset TI dengan suatu manajemen keamanan. Sumber data didapatkan dari studi pustaka, hasil wawancara dan pengamatan secara langsung. Melalui analisis ini didapatkan bahwa tingkat pengendalian manajemen keamanan PT Bank QNB Kesawan, Tbk berada pada level 1 (*Initial/Ad Hoc*) sampai level 4 (*Managed and Measurable*).

Kata kunci: COBIT 4.1, Audit Sistem Informasi, Manajemen Keamanan, Domain DS 5

ABSTRACT

Information Technology (IT) is becoming an integral part of and integrated with an organization's business objectives. With the help of IT, business processes that occur in the organization can be done quickly and efficiently. In addition to facilitate the enterprise, information technology does not escape from the threat of physical and non-physical. To prevent those threats companies need to conduct analysis and periodic evaluations. In this report, the case was taken Bank QNB Kesawan. The theory used the COBIT 4.1 domain Deliver and Support (DS) 5 Ensure System Security. Domain DS 5 is about the need to maintain the integrity of information and protect IT assets with a security management. Source data obtained from the literature, interviews, and observation directly. Through this analysis it was found that the level of security management controls PT Bank QNB Kesawan, Tbk is at level 1 (Initial/Ad Hoc) until level 4 (Managed and Measurable).

Keywords: COBIT 4.1, Information Systems Audit, Security Management, Domain DS 5

DAFTAR ISI

PRAKATA.....	i
ABSTRAK.....	iii
ABSTRACT	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR	vi
DAFTAR TABEL	vii
DAFTAR LAMPIRAN	viii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup Kajian	2
1.5 Sumber Data	3
1.6 Sistematika Penyajian	3
BAB II KAJIAN TEORI	5
2.1 Pengertian Sistem Informasi dan Teknologi Informasi.....	5
2.2 <i>Flowchart</i>	6
2.3 Pengertian Audit Sistem Informasi.....	10
2.4 COBIT 4.1.....	11
2.4.1 <i>Plan and Organise (PO)</i>	16
2.4.2 <i>Acquire and Implement (AI)</i>	23
2.4.3 <i>Deliver and Support (DS)</i>	28
2.4.4 <i>Monitor and Evaluate (ME)</i>	35
2.5 Penjelasan Kontrol Objektif DS5.....	38
2.6 Model Kematangan (<i>Maturity Models</i>).....	40
BAB III ANALISIS DAN EVALUASI	44
3.1 Profil Perusahaan.....	44
3.1.1 Visi dan Misi Perusahaan	45
3.1.2 Struktur Organisasi	46
3.2 Penjelasan Sistem Informasi	49
3.2 Proses Bisnis.....	50
3.3 <i>Flowchart</i>	51
3.4 Proses COBIT 4.1 Domain DS 5 <i>Ensure System Security</i>	52
BAB IV SIMPULAN DAN SARAN.....	67
4.1 Simpulan.....	67
4.2 Saran	69
DAFTAR PUSTAKA.....	70
RIWAYAT HIDUP PENULIS	71
LAMPIRAN	A.1

DAFTAR GAMBAR

Gambar 1. COBIT 4.1	12
Gambar 2. Fokus pada Bisnis	13
Gambar 3. Domain COBIT 4.1	14
Gambar 4. Batasan Bisnis, Umum, dan Kontrol Aplikasi	15
Gambar 5. Model Kematangan (<i>Maturity Models</i>)	16
Gambar 6. Struktur Organisasi PT Bank QNB Kesawan, Tbk.....	48
Gambar 7. Aplikasi <i>Equation</i>	49
Gambar 8 <i>Flowchart</i>	51
Gambar 9. Tampilan Awal <i>Equation</i>	B.1
Gambar 10. Menu Utama <i>Customer Service</i>	B.2
Gambar 11. Memo <i>Internal</i> Permohonan Pembuatan <i>User ID dan Password</i>	C.1
Gambar 12. Prosedur Persetujuan Pemilik Sistem dalam Pemberian Hak Akses.....	C.2
Gambar 13 Surat Pernyataan Untuk Menjaga Kerahasiaan Data Perusahaan	C.3
Gambar 14. Tabung Pemadam Kebakaran	D.1
Gambar 15. <i>Hydrant</i>	D.2
Gambar 16. <i>Emergency Door Release</i>	D.2
Gambar 17. <i>Fire Sprinkler System</i>	D.3
Gambar 18. Sistem Kartu Penguncian Pintu.....	E.1
Gambar 19. Perbedaan Hak Akses <i>User</i> ke <i>Server</i>	F.1
Gambar 20. Hak Akses <i>User</i> ke PC	F.2
Gambar 21. Hak Akses <i>User</i> ke Aplikasi Web	F.2
Gambar 22 User Akses Level Ke Sistem <i>Equation</i>	F.3
Gambar 23 Hak Akses <i>User</i> Ke Dalam Sistem.....	F.4
Gambar 24 Antivirus McAfee.....	G.1
Gambar 25 Antivirus McAfee (<i>On Access Scan Properties</i>).....	G.2
Gambar 26 Antivirus McAfee (<i>On Demand Scan Properties</i>).....	G.3
Gambar 27 <i>Malicious Software Prevention</i>	G.4
Gambar 28 <i>Malicious Software Correction</i>	G.5
Gambar 29 Dokumentasi Penanganan Masalah Sistem Informasi	H.1
Gambar 30 Pendefinisian Kemungkinan Permasalahan Sistem Informasi	H.2
Gambar 31 Cara Penyelesaian Masalah Sistem Informasi	H.3
Gambar 32 Dokumentasi Permasalahan Sistem Informasi	H.4
Gambar 33 Prosedur Tata Kelola <i>Firewall</i>	I.1
Gambar 34 Intranet Bank Kesawan	J.1
Gambar 35 Prosedur Pengelolaan Kunci.....	K.1

DAFTAR TABEL

Tabel I. <i>Flow Direction Symbols</i>	7
Tabel II. <i>Processing Symbols</i>	8
Tabel III. <i>Input / Output Symbols</i>	9
Tabel IV. <i>DS 5.1 Management of IT Security</i>	52
Tabel V. <i>DS 5.2 IT Security Plan</i>	53
Tabel VI. <i>DS 5.3 Identity Management</i>	55
Tabel VII. <i>DS 5.4 User Account Management</i>	56
Tabel VIII. <i>DS 5.5 Security Testing, Surveillance, and Monitoring</i>	57
Tabel IX. <i>DS 5.6 Security Incident Definition</i>	59
Tabel X. <i>DS 5.7 Protection of Security Technology</i>	60
Tabel XI. <i>DS 5.8 Cryptographic Key Management</i>	61
Tabel XII. <i>DS 5.9 Malicious Software Prevention, Detection, and Correction</i>	62
Tabel XIII. <i>DS 5.10 Network Security</i>	64
Tabel XIV. <i>DS 5.11 Exchange of Sensitive Data</i>	65

DAFTAR LAMPIRAN

Lampiran A Wawancara.....	A.1
Lampiran B Sistem Equation.....	B.1
Lampiran C <i>User Account Management</i>	C.1
Lampiran D <i>Protection of Security Technology</i>	D.1
Lampiran E <i>Security Testing, Surveillance, and Monitoring</i>	E.1
Lampiran F <i>Identity Management</i>	F.1
Lampiran G <i>Malicious Software Prevention, Detection, and Correction</i>	G.1
Lampiran H <i>Security Incident Definition</i>	H.1
Lampiran I <i>Network Security</i>	I.1
Lampiran J <i>Exchange Sensitive Data</i>	J.1
Lampiran K <i>Cryptographic Key Management</i>	K.1