Manajemen Risiko Teknologi Informasi Berbasis National Institute of Standards and Technology Sp800-30 di Universitas Jenderal Achmad Yani

Ae Saepul, Yulison Herry C, Asep Id Hadiana
Jurusan Informatika, Fakultas MIPA
Universitas Jenderal Achmad Yani
Jl. Terusan Sudirman, Cimahi
aesaepul3411131097@gmail.com, ahadiana@gmail.com

***Abstrak*—Sebagai sebuah lembaga pendidikan Universitas Jenderal Achmad Yani tentunya memanfaatkan teknologi informasi untuk menunjang keberlangsungan sistem informasi yang sedang berjalan. Bagi Unjani teknologi informasi merupakan salah satu bagian terpenting dalam pengelolaan sistem informasi, dimana keberhasilan pelayanan perguruan tinggi salah satunya bergantung pada sejauh mana pengelolaan terhadap teknologi informasi yang sudah dilakukan. Akan tetapi dalam penggunaan teknologi Informasi tidak selamanya berjalan sesuai harapan, dalam proses penggunaannya seringkali muncul risiko – risiko yang dapat mengganggu keberlangsungan sistem informasi tersebut sehingga dapat menyebabkan kerugian baik kerugian material maupun nonmaterial. Sehingga manajemen risiko teknologi informasi sangat penting untuk diterapkan di Universitas Jenderal Achmad Yani, karena dengan adanya penerapan mnajemen risiko diharapkan dapat mengurangi risiko yang akan terjadi pada teknologi informasi. Penilaian risiko di Unjani ini akan dilaksanakan dengan menggunakan kerangka kerja NIST Sp800-30, tujuan dari penilaian risiko ini yaitu untuk mendefinisikan risiko yang mungkin terjadi pada teknologi informasi di Universitas Jenderal Achmad Yani serta memberikan rekomendasi kontrol untuk pencegahan risiko tersebut.**

Kata kunci— manajemen risiko, Information Technology, NIST Sp800-30.

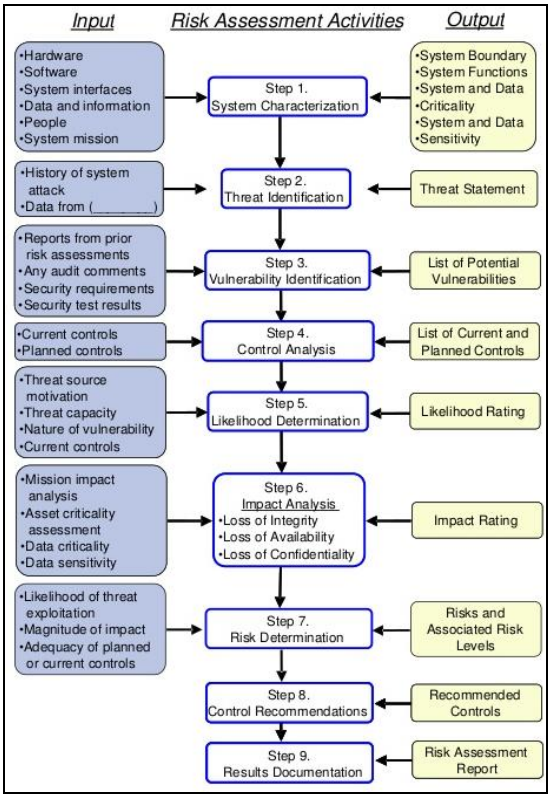
I. PENDAHULUAN

Universitas Jenderal Achmad Yani adalah sebuah perguruan tinggi dibawah naungan Yayasan Kartika Eka Paksi yang terletak di Bandung dan Cimahi. Universitas Jenderal Achmad Yani ini memiliki 7 fakultas dan memiliki 23 jurusan. Sebagai sebuah lembaga pendidikan tentunya mempunyai sistem informasi untuk membantu tercapainya rencana strategi lembaga tersebut. Untuk menjalankan sistem informasi UNJANI tentunya memiliki teknologi informasi. Dalam penggunaan teknologi informasi tersebut tentunya tidak lepas dari risiko yang mungkin akan timbul dan dapat mengancam asset yang dimiliki baik material maupun nonmaterial, seperti yang pernah terjadi pada 6 tahun terakhir yaitu kegagalan sistem yang disebabkan oleh tidak berfungsinya data center Unjani karena aliran listrik utama dari PLN terputus dan tidak ada sumber listrik cadangan ketika aliran listrik utama terputus. Untuk meminimalisir risiko perlu adanya penerapan manajemen risiko agar risiko tersebut dikelola dan dicari langkah pencegahan yang tepat dengan menggunakan kerangka kerja tertentu.

Manajemen risiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman; suatu rangkaian aktivitas manusia termasuk: Penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan / pengelolaan sumberdaya [1]. Manajemen risiko bisa diterapkan diterapkan diberbagai bidang salah satunya pada bidang teknologi informasi [2]. NIST atau National Institute of Standards and Technology merupakan organisasi pemerintah di Amerika Serikat yang menyusun panduan pada bidang teknologi informasi. National Institute of Standards and Technology, disingkat NIST (Badan Nasional Standar dan Teknologi Amerika Serikat) yang dulunya dikenal sebagai The National Bureau of Standards - NBS (Biro Standar Nasional) adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat. Misi dari badan ini adalah untuk membuat dan mendorong pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang [3]. NIST telah mempublikasikan NIST Special Publication 800-30 yang berjudul "Risk Management Guide for Information Technology" [4]. Penelitian terdahulu yang pernah dilakukan yaitu manajemen risiko pada sistem informasi perguruan tinggi menggunakan kerangka kerja NIST SP800-30. Tujuan dari penelitian ini yaitu untuk meningkatkan efektivitas biaya yang dikeluarkan oleh organisasi guna memastikan keamanan dari sistem teknologi informasi yang digunakan. Sehingga dapat dipastikan asset teknologi informasi yang dimiliki oleh organisasi seluruhnya aman dari berbagai gangguan maupun ancaman yang dapat merusaknya, baik gangguan dari pihak internal maupun pihak external [5]. Pemilihan kerangka kerja ini atas dasar penelitian sebelumnya yang menggunakan kerangka kerja NIST Sp800-30 sebagai kerangka kerja penilaian risiko teknologi informasi di perguruan tinggi dengan hasil berupa dokumentasi berupa profil risiko yang dapat mengancam keberlangsungan sistem informasi dan solusi pencegahan melalui rekomendasi kontrol sebagai tindak lanjut proses berikutnya melalui kegiatan mitigasi risiko.

II. METODE

NIST atau *National Institute of Standards and Technology* merupakan organisasi pemerintah di Amerika Serikat yang menyusun panduan pada bidang teknologi informasi. *National Institute of Standards and Technology*, disingkat NIST (Badan Nasional Standar dan Teknologi Amerika Serikat) yang dulunya dikenal sebagai *The National Bureau of Standards - NBS* (Biro Standar Nasional) adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat [6]. Misi dari badan ini adalah untk membuat dan mendorong untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang [7]. NIST telah mempublikasikan NIST *Special Publication* 800-30 yang berjudul *"Risk Management Guide for Information Technology Sistems"*. Proses NIST Sp800-30 dapat dilihat pada Gambar 1 [8].



Gambar 1. NIST Sp800-30.

Proses penilaian risiko dalam NIST Sp800-30 ini sebagai berikut :

A. *System Characterization*

Langkah pertama dalam menilai risiko adalah untuk menentukan ruang lingkup usaha. Untuk melakukan hal ini, mengidentifikasi di mana dibuat, diterima, dipelihara, diproses, atau ditransmisikan.

B. *Threat Identification*

Untuk langkah ini, potensi ancaman (potensi sumber ancaman untuk berhasil melaksanakan kerentanan tertentu) diidentifikasi dan didokumentasikan. Sumber ancaman adalah setiap keadaan atau peristiwa dengan potensi untuk menyebabkan kerusakan pada sistem IT (disengaja atau tidak disengaja).

C. *Vulnerability Identification*

Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem teknis dan non-teknis (kekurangan atau kelemahan) yang dapat dimanfaatkan atau dipicu oleh sumber-sumber ancaman - potensial.

D. *Control Analysis*

Tujuan dari langkah ini adalah untuk mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (probabilitas) dari sumber ancaman – mengeksploitasi kerentanan sistem.

E. *Likelihood Determination*

Tujuan dari langkah ini adalah untuk menentukan nilai keseluruhan kemungkinan yang menunjukkan kemungkinan bahwa kerentanan dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan yang ada atau yang direncanakan.

F. *Impact Analysis*

Tujuan dari langkah ini adalah untuk menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman yang berhasil mengeksploitasi kerentanan.

G. *Risk Determination*

Menghitung level risiko dengan mengalikan peringkat dari penentuan kemungkinan dan analisis dampak.

H. *Control Recommendations*

Tujuan dari langkah ini adalah untuk mengidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi, sesuai dengan operasi organisasi.

I. *Result Documentation*

Penyusunan laporan keseluruhan proses penilaian risiko

III. HASIL DAN DISKUSI

A. *System Characterization*

Karakteristik teknologi informasi di Unjani yaitu: *bandwidth* sebesar 100mbps, sistem operasi *server* menggunakan *linux Ubuntu server*, *database* yang digunakan yaitu *mysql*, data yang ada di Unjani yaitu : data PMB, akademik, keuangan, kepegawaian dan perpustakaan, sistem informasi yang ada di Unjani di antaranya : SI Penerimaan Mahasiswa Baru (PMB)

a. SI Akademik (SIAKAD)
b. SI Keuangan dan Akuntansi (SISKA)
c. SI Kepegawaian
d. SI Perpustakaan

B. Threat Identification

Berikut beberapa sumber ancaman yang teridentifikasi dapat mengganggu teknologi informasi pada Universitas Jenderal Achmad Yani pada Tabel 1.

TABEL 1. SUMBER ANCAMAN.

No	Sumber ancaman
1	Aliran listrik
2	Gempa bumi
3	Kebakaran
4	Banjir
5	Jaringan komputer
6	Virus, hacking, malware
8	Manusia

C. Vulnerability Identification

Berikut adalah kerentanan dari teknologi informasi di Unjani pada Tabel 2.

TABEL 2. IDENTIFIKASI ANCAMAN.

No	Kerentanam	Ancaman
1	Belum memasang anti petir.	Perangkat tersambar petir sehingga mengalami kerusakan.
2	Tidak ada fasilitas *detector* kebakaran & fasilitas pencegahannya.	Ketika terjadi kebakaran api sulit untuk dipadamkan dan memungkinkan api tersebut menjalar ke berbagai perangkat lainnya.
3	Sumber listrik cadangan terbatas.	Ketika sumber listrik cadangan mati / habis data center tidak dapat beroperasi.
4	Lokasi data center terletak diatas kantin & dekat dengan tempat umum.	Memungkinkan terjadinya kebakaran yang bersumber dari kantin yang berada dibawah data center dan masuk debu dari ventilasi udara.
5	Memakai plafon gypsum.	Kerusakan pada perangkat yang ada di data *center* karena terjadi kebocoran pada saat hujan.
6	Kurangnya pengamanan data *center*.	Kehilangan perangkat pada data *center* karena belum ada fasilitas cctv untuk memantau ruangan data center dan tidak ada hak akses khusus untuk memasuki ruangan data center.
7	*Bandwith* kecil.	Lambatnya akses jaringan karena bandwith yang tersedia kecil.
8	*Maintenance* oleh pihak ke 3.	Kemungkinan terjadinya sabotase atau pencurian data oleh pihak ke 3.
9	Perangkat yang ada belum terdokumentasi sepenuhnya.	Kesulitan saat mengganti perangkat yang rusak.
10	Struktur bangunan tidak kokoh.	Pada saat terjadi gempa bumi dengan skala menengah keatas kemungkinan akan terjadi kerusakan berat pada data center.
11	Belum ada prosedur mengenai staff pengelola IT yang keluar / pension.	Kemungkinan staff tersebut masih memiliki hak akses informasi dan berisiko penyalahgunaan, pencurian / modifikasi data.

D. Control Analysis

Berikut adalah pengendalian yang diterapkan oleh pihak pengelola TI Unjani dapat dilihat pada Tabel 3:

TABEL 3. IDENTIFIKASI PENGENDALIAN.

No	Ancaman	Pengendalian
1	Listrik PLN mati.	Memasang UPS untuk s*upply* listrik cadangan.
2	Server akademik rusak / kesalahan fungsi.	Mendatangkan pihak ke 3 untuk memperbaiki server akademik.
3	Server lain rusak.	Diperbaiki oleh pihak Internal.
4	Kerusakan komponen TI.	Diperbaiki oleh pihak Internal.
5	Kehilangan data.	Melakukan backup data secara berkala.

E. Likelihood Determination

Penentuan kemungkinan risiko ini dihitung berdasarkan rumus likert dengan mengalikan jumlah jawaban dengan bobot dibagi jumlah responden [9]. Hasil perhitungan tersebut terdapat pada Tabel 4.

$$rata - rata\ jawaban = \frac{\sum(jawaban\ x\ bobot)}{\sum responden} \quad (1)$$

TABEL 4. PENENTUAN KEMUNGKINAN RISIKO.

No	Pernyataan	Rata – rata
1	P1	0.43
2	P2	0.59
3	P3	0.3
4	P4	0.24
5	P5	0.19
6	P6	0.52
7	P7	0.34
8	P8	0.94
9	P9	0.18
10	P10	0.51
11	P11	0.2
12	P12	0.33
13	P13	0.27

No	Pernyataan	Rata – rata
14	P14	0.32
15	P15	0.37
16	P16	0.33
17	P17	0.34
18	P18	0.23
19	P19	0.2
20	P20	0.27
21	P21	0.52
22	P22	0.51
23	P23	0.18
24	P24	0.23
25	P25	0.18
26	P26	0.14
27	P27	0.42
28	P28	0.42
29	P29	0.44
30	P30	0.24

F. Impact Analysis

Rata – rata dampak dihitung berdasarkan Persamaan 1, hasilnya perhitungan tersebut terdapat pada Tabel 5 :

TABEL 5. PERHITUNGAN DAMPAK.

No	Pernyataan	Rata – rata
1	P1	90
2	P2	100
3	P3	74.44
4	P4	54.44
5	P5	54.44
6	P6	80
7	P7	90
8	P8	100
9	P9	57.78
10	P10	62.22
11	P11	43.33
12	P12	57.78
13	P13	52.22
14	P14	52.22
15	P15	57.78
16	P16	52.22
17	P17	63.33
18	P18	32.22
19	P19	33.33
20	P20	77.78
21	P21	23.33
22	P22	48.89
23	P23	52.22
24	P24	58.89
25	P25	42.22
26	P26	52.22
27	P27	48.89
28	P28	54.44
29	P29	52.22
30	P30	28.89

G. Risk Determination

Level risiko adalah hasil pembulatan dari hasil perhitungan Persamaan 2. Hasil perhitungan Persamaan 2 terdapat pada Tabel 6.

Penilaian Risiko = Dampak x Peluang (2)

TABEL 6. LEVEL RISIKO.

No	Pernyataan	Level risiko
1	P1	Medium
2	P2	High
3	P3	Medium
4	P4	Medium
5	P5	Low
6	P6	Medium
7	P7	Medium
8	P8	High
9	P9	Low
10	P10	Medium
11	P11	Low
12	P12	Medium
13	P13	Medium
14	P14	Medium
15	P15	Medium
16	P16	Medium
17	P17	Medium
18	P18	Low
19	P19	Low
20	P20	Medium
21	P21	Medium
22	P22	Medium
23	P23	Low
24	P24	Medium
25	P25	Low
26	P26	Low
27	P27	Medium
28	P28	Medium
29	P29	Medium
30	P30	Low

H. Control Recommendations

Tujuan dari kontrol ini adalah untuk mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima. Rekomendasi kontrol dapat dilihat pada Tabel 7.

TABEL 7. REKOMENDASI KONTROL YANG DIAJUKAN.

No	Pernyataan	Rekomendasi kontrol
1	P1	- Memasang UPS dengan kemampuan backup daya selama >5 jam. - Membuat jalur listrik cadangan dari genset.
2	P2	- Melakukan pemeriksaan kabel listrik secara berkala, sebaiknya dilakukan satu kali dalam satu bulan. - Memasang *Mini Circuit Breaker* untuk mencegah konsleting listrik. - Mengasuransikan peralatan teknologi informasi yang digunakan.
3	P3	- Melakukan pemeriksaan kabel dan sumber listrik cadangan secara berkala, sebaiknya dilakukan satu kali dalam satu tahun. - Memasang *Mini Circuit Breaker* untuk mencegah konsleting listrik.
4	P4	- Memberi lapisan tambahan khususnya untuk kabel supaya jika tergenangi air tidak mengalami kerusakan / konslet. - Pembuatan mirroring server.
5	P5	- Melakukan backup data secara berkala. - Memperbaiki susunan ruangan data

No	Pernyataan	Rekomendasi kontrol
		center supaya tahan terhadap gempa diatas 5 skala richter. - Mengasuransikan peralatan teknologi informasi yang digunakan. - Pembuatan mirroring server.
6	P6	- Menambahkan fasilitas detector api agar mudah mendeteksi api. - Menambah fasilitas pemadam api. - Melakukan pengecekan secara berkala untuk mencegah timbulnya percikan api baik itu dari konsleting listrik, dll.
7	P7	- Menambah fasilitas pemadam api. - Mengasuransikan peralatan teknologi informasi yang digunakan. - Pembuatan mirroring server.
8	P8	- Memasang penangkal petir. - Mengasuransikan peralatan teknologi informasi yang digunakan.
9	P9	- Menutup ventilasi udara yang langsung menghadap ke luar ruangan. - Mengasuransikan peralatan teknologi informasi yang digunakan.
10	P10	- Melakukan pengecekan jaringan secara berkala sebaiknya dilakukan satu kali dalam sebulan.
11	P11	- Menambah fasilitas kemanan, seperti: cctv.
12	P12	- Menggunakan firewall atau anti virus. - Melakukan backup secara otomatis ketika data itu disimpan.
13	P13	- Menggunakan firewall. - Membatasi akses terhadap informasi rahasia.
14	P14	- Mengamankan data rahasia - Melindungi dari akses illegal
15	P15	- Melakukan backup data secara berkala.
16	P16	- Menambah fasilitas kemanan seperti cctv.
17	P17	- Memasang anti virus / firewall.
18	P18	- Menghapus hak akses pengguna / karyawan yang sudah pension / tidak bekerja lagi.
19	P19	- Menutup ventilasi udara.
20	P20	- Memantau proses perbaikian. - Melatih SDM.
21	P21	- Membuat SOP penggunaan TI.
22	P22	- Menambah bandwith.
23	P23	- Meninjau kembali SOP mengenai penetimaan SDM. - Memperbaiki susunan kepegawaian SDM berdasarkan kemampuan.
24	P24	- Membatasi hak akses informasi yang bersifat rahasia. - Memasang firewall.
25	P25	- Membatasi hak akses.
26	P26	- Melakukan pengecekan secara berkala pada masing – masing komponen teknologi informasi. - Jika perawatan tidak memungkinkan oleh pihak internal, pengelola bisa melakukan outsourching.
27	P27	- Mengasuransikan peralatan teknologi informasi yang digunakan. - Memonitoring penggunaan teknologi informasi.
28	P28	- Memasang anti virus. - Memasang firewall. - Jika sudah terpasang antivirus, perbaharui antivirus tersebut jika ada perbaharuan terbaru.
29	P29	- Melakukan monitoring berkala yang dilakukan beberapa kali dalam seminggu. - Jika tidak memungkinkan diperbaiki oleh pihak internal, pengelola bisa melakukan outsourching untuk memperbaikinya.
30	P30	- Mengecek fasilitas pendukung yang menunjang berjalannya teknologi informasi.

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan mengenai manajemen risiko teknologi informasi di Unjani, diperoleh hasil 2 risiko level tinggi, 19 risiko level sedang dan 9 risiko level risiko rendah. Risiko level tinggi ini bersumber dari bencana alam dan dari sumber listrik yaitu kerusakan infrastruktur teknologi informasi akibat tersambar petir dan kerusakan akibat fluktuasi / konsleting listrik dari sumber listrik utama yaitu dari PLN. Berdasarkan penilaian kemungkinan terjadi risiko kerusakan yan diakibatkan oleh sambaran petir adalah risiko kerusakan yang paling sering terjadi dikarenakan belum dipasangnya penangkal petir.

DAFTAR PUSTAKA

[1] E. Pujastuti, A. Nasiri, "Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi "SMART PMB" di STMIK AMIKON Yogyakarta," In *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, (pp. 1-7). Yogyakarta, 2016.

[2] I. Masyhuti, F. Samopa, "Pengembangan manajemen risiko teknologi informasi pada sistem penerimaan peserta didik baru (PPDB Online) Kemendikbuf menggunakan framework NIST Sp800-30," *Seminar Nasional manajemen Teknologi XVIII 2013*, (pp. c.6-1 - c.6-6). Surabaya. 2013.

[3] A. Nurochman, "Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Gadjah mada Yogyakarta)," *Berkala Ilmu Perpustakaan dan Informasi*, Yogyakarta, 2014.

[4] U. Nugraha, "Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST Sp 800-30," *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, Bandung. 2016.

[5] Y. Gerhana, A. Erdiansyah, U. Syarifudin, "Penilaian Risiko Teknologi Informasi & Keamanan Sistem Informasi dengan Menggunakan COBIT 4.1 dan Guildlines NIST Sp800-30 (Studi Kasus Rumah Sakit Dr Slamet Garut)," *Berkala Ilmu Perpustakaan dan Informasi* (No. 1-2), 161-169. 2016.

[6] G. Stoneburner, A. Goguen, A. Feringa, "Recommedation of National Institute of Standards and Technology Special Publication 800-30," *Risk Management Guide for Information Technology System*, 2001.

[7] H. S. Firmansyah, "Implementasi Framework Manajemen Risiko Terhadap Penggunaan Teknologi Informasi Perbankan," 172-178. Oktober .2009.

[8] M. I. Andani, "Manajemen Risiko Keamanan Aplikasi Sistem Informasi Laporan Harian PKS & PPKO Online pada PTPN V Menggunakan Metode NIST SP800-30," *Jurnal Ilmiah Media Enginering*.

[9] W. Widhiarso, SKALA LIKERT (Summated Ratings), *Fakultas Psikologi UGM*.

[10] S. Dharwiyanti, Satria R. Wahono, "Pengantar Unified Modeling Language (UML)," *IlmuKomputer.Com*, 2003.

[11] B. N. Pujiono, I. Tama, R. Efranto, "Analisis Potensi Bahaya Serta Rekomendasi Perbaikan Dengan Metode Hazard And Operability Study (HAZOP) Melalui Perangkingan OHS Risk Assesment And Control," Malang, 2016.

[12] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[13] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[14] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.