

**MANAJEMEN RISIKO SISTEM INFORMASI PERPUSTAKAAN
(STUDI KASUS DI PERPUSTAKAAN
UNIVERSITAS GADJAH MADA YOGYAKARTA)**

Arif Nurochman
arif.nurochman@mail.ugm.ac.id

Abstract

Library information systems and information assets administered to users become the backbone of library service with the support of information technology. However, the application of library information systems that grows rapidly may raise the risk that causes failures threatening librarians in assessing sources of risk threats. Risks may include events and conditions that lead to disruption in information services and the problem of the decision-making process. evaluation although not documented in writing. Informants of this study consist of librarians who have social interaction with library information system. The method uses qualitative case study approach with in-depth interviews and direct observation.

The results of the study identifies the risk in a hang of backup server is high, i

The purpose of this study is to describe the implementation of risk management in information systems at Gadjah Mada University Library using NIST SP 800-30 framework and to determine factors that affect the implementation of risk management in information systems at the library. Risk management in information systems at Gadjah Mada University Library has been implemented to anticipate the various sources of risk threats by conducting risk assessment, risk mitigation and risk n electricity is high, in security systems is high, in passwords is high, in authorization permission is moderate and in human resources is moderate. To reduce and eliminate the risk impact, Gadjah Mada University Library conducts risk mitigation by transferring the risk from a library information system servers to PSDI (Center for Systems and Information Resources), while the risk evaluation of the activities is carried out continuously and consistently by the librarians to implement control and activities in risk mitigation to the extent acceptable to the library. Factors affecting the implementation of risk management information systems at the Gadjah Mada University Library are influenced by the policies of the University, the perception of the library's head and human resources and technical capabilities in the field of information technology.

Keywords: Risk Management, Library Information Systems, NIST SP 800-30 Framework

Abstrak

Sistem dan aset informasi perpustakaan yang dilayankan kepada pemustaka menjadi tulang punggung dengan adanya peran teknologi informasi. Penerapan sistem informasi perpustakaan yang berkembang pesat menimbulkan risiko yang dapat mengancam disebabkan kegagalan pustakawan dalam menilai sumber ancaman risiko. Risiko dapat berupa kejadian dan kondisi yang mengakibatkan dampak layanan informasi menjadi terganggu dan berhentinya proses pengambilan keputusan. Tujuan penelitian ini untuk mendeskripsikan pelaksanaan manajemen risiko sistem informasi perpustakaan di Perpustakaan Universitas Gadjah Mada (UGM) dengan menggunakan kerangka kerja (*framework*) NIST SP 800-30 dan untuk mengetahui faktor-faktor yang mempengaruhi pelaksanaan manajemen risiko sistem informasi perpustakaan. Manajemen risiko sistem informasi perpustakaan di Perpustakaan UGM telah dilaksanakan untuk mengantisipasi berbagai sumber ancaman risiko dengan melaksanakan kegiatan penilaian risiko, peringanan risiko dan evaluasi risiko meskipun tidak

didokumentasikan secara tertulis. Informan penelitian terdiri atas pustakawan yang memiliki situasi sosial berinteraksi dengan sistem informasi perpustakaan. Menggunakan metode kualitatif, pendekatan studi kasus dengan wawancara mendalam dan pengamatan langsung (observasi). Hasil penelitian teridentifikasi level penilaian risiko berupa backup server high risiko tinggi, listrik risiko tinggi, keamanan sistem risiko tinggi, password risiko tinggi, otorisasi hak akses risiko sedang dan sumber daya manusia risiko sedang.

Untuk mengurangi dan menghilangkan dampak risiko, Perpustakaan UGM melaksanakan kegiatan peringanan risiko (mitigasi) dengan memindahkan risiko berupa *server* sistem informasi perpustakaan ke PSDI (Pusat Sistem dan Sumberdaya Informasi). Kegiatan evaluasi risiko dilaksanakan secara terus menerus dengan konsistensi dari pustakawan untuk melaksanakan kegiatan rekomendasi kontrol peringanan risiko sampai pada tahap yang dapat diterima oleh perpustakaan. Faktor yang mempengaruhi pelaksanaan manajemen risiko sistem informasi di Perpustakaan UGM dipengaruhi oleh kebijakan dari lembaga universitas, persepsi kepala perpustakaan dan kemampuan sumber daya manusia yang memiliki kemampuan teknis dalam bidang teknologi informasi.

Kata Kunci: Manajemen Risiko, Sistem Informasi Perpustakaan, *Framework* NIST SP 800-30

PENDAHULUAN

Undang-Undang Nomor 43 Tahun 2007 tentang perpustakaan menyebutkan bahwa perpustakaan adalah institusi pengelola koleksi karya tulis, karya cetak, dan/atau karya rekam secara profesional dengan sistem yang baku guna memenuhi kebutuhan pendidikan, penelitian, pelestarian, informasi, dan rekreasi para pemustaka. Pada kondisi sekarang pemustaka utamanya masyarakat terbiasa dengan nilai informasi yang dipengaruhi oleh sinergi antara perangkat teknologi informasi, teknologi *web* dan sumber-sumber informasi global yang tersedia di internet.

Pemenuhan kebutuhan informasi di mana dan kapan saja tanpa batas ruang dan waktu menjadi tolok ukur mengingat jaman sekarang disebut dengan *'the age of network intelligence'*, yang dibackup oleh jaringan informasi modern sehingga segala urusan dapat dilakukan tanpa harus berada di tempat kegiatan dilaksanakan (Supriyanto, 2008:147). Kolaborasi informasi dengan perangkat teknologi *web* memungkinkan kecepatan dan keakuratan informasi menjadi tujuan utama, maka tidak mengherankan apabila muncul istilah di masyarakat siapa yang menguasai informasi maka dipastikan ia memiliki keunggulan posisi dalam persaingan global (Setiarso, 1997:24). Saat ini karakteristik pemustaka perguruan tinggi lebih menggantungkan pada informasi terkini. Hal ini menjadi *euforia* yang dilatarbelakangi oleh maraknya pengembangan konsep perpustakaan berbasis digital. Berbagai aspek pembahasan bergulir dengan cepat, salah satu yang berkembang

menjadi bahan diskusi adalah tersedianya sistem informasi perpustakaan yang digunakan untuk menseleksi, menyimpan, mengolah, dan melayani informasi kepada pemustaka dengan menggunakan teknologi *web*. Sifat teknologi *web* yang mudah diakses dan digunakan menjadi alasan utama dipilih perpustakaan perguruan tinggi untuk pelayanan informasi perpustakaan.

Ketika transformasi layanan perpustakaan yang bersifat *"book-centric"* berubah kearah *"user-centric"* dengan penerapan teknologi *web*, perpustakaan tanpa sadar meninggalkan kegiatan pengelolaan aset informasi beserta sistem informasi sebagai sarana utama dalam memberikan layanan kepada pemustaka. Teknologi *web* memberikan kemudahan untuk mengakses informasi cepat dan murah yang disediakan oleh *website* maupun pustaka digital. Selain manfaat berupa kecepatan dan kemudahan akses, teknologi *web* rentan terhadap *sabotase* serta tindak kejahatan (Suduc, 2010). Apabila terjadi hal yang demikian maka sistem informasi perpustakaan tidak bisa memproses, menyimpan dan mendistribusikan informasi kepada pemustaka dan perpustakaan.

Berbagai macam hambatan yang mengganggu sistem informasi umumnya disebut sebagai risiko. Risiko dapat terdiri dari berbagai macam kejadian dan kondisi yang berhubungan dengan sistem informasi perpustakaan yang berdampak negatif bagi perpustakaan. Perpustakaan belum melaksanakan kegiatan penilaian risiko pada sistem informasi yang digunakan, sedangkan sistem informasi dan

teknologi *web* hanya sebatas sebagai sarana layanan informasi tanpa melaksanakan tindakan pencegahan ancaman risiko yang setiap saat mengancam berjalannya sistem informasi. Di satu sisi, sistem informasi perpustakaan telah menjadi bagian yang sulit dipisahkan dalam setiap kegiatan layanan dan proses pengelolaan yang dilakukan oleh perpustakaan. Apabila terjadi gangguan pada sistem informasi perpustakaan maka layanan informasi menjadi terganggu yang mengakibatkan keberlangsungan sistem kerumahtanggaan perpustakaan menjadi terhenti.

Perpustakaan Universitas Gadjah Mada (UGM) telah mengaplikasikan sistem informasi yang dilatarbelakangi oleh pengetahuan, perkembangan ilmu dan teknologi. Implikasi dari penerapan teknologi informasi tersebut menempatkan UGM sebagai perguruan tinggi negeri di Indonesia beserta perpustakaanannya menempati posisi pertama penilaian *webometric* untuk pemeringkatan *world ranking of word university* (Muntashir, 2012:47).

Berdasarkan observasi pendahuluan yang dilaksanakan sebelumnya, Perpustakaan UGM mengklasifikasikan kejadian dan sumber risiko yang berkaitan dengan sistem informasi beserta aset-aset teknologi informasi merupakan tanggung jawab lembaga universitas yang memiliki kewenangan dalam hal pengelolaan teknologi informasi yakni PSDI (Pusat Sistem dan Sumber Daya Informasi) bukan menjadi tanggung jawab perpustakaan. Perpustakaan UGM belum melaksanakan kegiatan penilaian risiko tetapi hanya melaksanakan kegiatan berdasarkan kejadian "*eksidental*" yang saat itu terjadi terkait dengan layanan informasi perpustakaan. Meskipun secara struktur organisasi di Perpustakaan UGM terdapat bidang khusus yang menangani permasalahan yang berkaitan dengan teknologi informasi yakni bidang *database* dan jaringan. Karena kewenangan yang luas maka kegiatan manajemen risiko belum dilaksanakan sesuai dengan prosedur standar baku dan hanya berjalan apa adanya.

Kegiatan penilaian risiko di Perpustakaan UGM hanya berdasarkan pada pengalaman dan pengetahuan pustakawan yang sebatas pada pengenalan teknologi informasi, belum dilaksanakan secara khusus. Semakin besar aset informasi yang dilayankan kepada pemustaka melalui teknologi *web*, semakin besar sumber ancaman yang akan mengganggu kelancaran sistem informasi perpustakaan.

Manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa, dampak terhadap finansial, menurunnya reputasi yang disebabkan oleh sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan (Maulana dan Supangkat, 2006).

Salah satu cara untuk melaksanakan kegiatan manajemen risiko teknologi informasi adalah dengan menggunakan metode atau framework penilaian risiko NIST (*National Institute of Standard and Technology*) SP 800-30 yang dapat diaplikasikan untuk menganalisis risiko sistem informasi perpustakaan. Bagi Perpustakaan UGM sendiri dengan struktur organisasi dan pemenuhan kebutuhan yang bertumpu pada sistem informasi terintegrasi, yang meliputi bidang pengadaan, pengolahan, layanan sirkulasi, penelusuran *Online Public Access Catalog* (OPAC), statistik dan administrasi perpustakaan yang masih mengalami perkembangan. Sehingga lebih cocok mengaplikasikan *framework* NIST SP 800-30 untuk menilai risiko dalam kegiatan manajemen risiko sistem informasi. *Framework* NIST SP 800-30 membahas manajemen risiko yang berhubungan dengan model proses analisis secara rinci dalam tingkat praktek manajemen sesuai dengan siklus hidup pengembangan sistem (*System Development Life Cycle*). *Framework* NIST SP 800-30 merupakan petunjuk yang mendeskripsikan metodologi manajemen risiko yang disesuaikan dengan fase siklus hidup pengembangan sistem dan bagaimana proses manajemen risiko terkait dengan proses otorisasi akreditasi (Stoneburner, 2002:4).

Untuk mengetahui proses penerapan manajemen risiko sistem informasi perpustakaan tersebut, diperlukan penelitian tentang sejauh mana penerapan manajemen risiko sistem informasi perpustakaan dalam menilai sumber ancaman dan kerentanan, menganalisis, mengurangi, serta mengevaluasi risiko terhadap aset informasi perpustakaan di Perpustakaan UGM.

Penelitian ini bertujuan untuk mendeskripsikan pelaksanaan manajemen risiko sistem informasi perpustakaan di Perpustakaan UGM dalam mengidentifikasi, menganalisis, mengelola evaluasi risiko dengan menggunakan *framework* NIST SP 800-30 dan untuk mengetahui faktor-faktor apa yang mempengaruhi pelaksanaan manajemen risiko sistem informasi perpustakaan.

TINJAUAN PUSTAKA

Pengertian risiko dan manajemen risiko

Definisi risiko menurut Pinontoan (2010:100) adalah akibat negatif dari sebuah kejadian atau suatu keputusan yang diambil dalam kehidupan sehari-hari. Darmawi (2006:1) mendefinisikan risiko sebagai kemungkinan akan terjadinya akibat buruk atau akibat yang merugikan, seperti kemungkinan kehilangan, cedera, kebakaran dan sebagainya. Dalam risiko tidak ada metode apapun yang bisa menjamin seratus persen bahwa akibat buruk itu setiap saat dapat dihindarkan, kecuali kalau kegiatan yang mengandung unsur risiko tidak dilakukan.

Sedangkan menurut Idroes (2008:4) menjelaskan risiko merupakan bahaya, risiko adalah ancaman atau kemungkinan suatu tindakan yang menimbulkan dampak yang berlawanan dengan tujuan yang ingin dicapai. Risiko merupakan peluang bagi organisasi untuk mencapai tujuannya dengan menerapkan konsep manajemen risiko yang sesuai dengan kebutuhan organisasi. Manajemen risiko didefinisikan sebagai suatu metode logis dan sistematis dalam identifikasi, kuantifikasi, menentukan sikap, menetapkan solusi, serta melakukan monitor dan pelaporan risiko yang berlangsung pada setiap aktivitas atau proses (Idroes, 2008:5).

Penerapan manajemen risiko dalam konteks organisasi adalah bagaimana suatu organisasi bisa mengelola risiko yang dihadapinya. Menurut Hanafi (2009:9) manajemen risiko pada dasarnya dilakukan melalui proses identifikasi risiko, evaluasi dan pengukuran risiko dan pengelolaan risiko. Organisasi sering kali secara sengaja mengoptimalkan risiko karena melihat potensi keuntungan dari risiko tersebut, sebaliknya apabila organisasi tidak dapat mengambil risiko maka dipastikan organisasi tersebut tidak dapat berkembang.

Djojosoedarso (1999:1) mendefinisikan manajemen risiko sebagai pelaksanaan fungsi-fungsi manajemen dalam penanggulangan risiko, terutama risiko yang dihadapi oleh organisasi/perusahaan, keluarga dan masyarakat. Manajemen risiko mencakup kegiatan merencanakan, mengorganisir, menyusun, memimpin/mengkoordinir dan mengawasi (termasuk mengevaluasi) program penanggulangan risiko. Senada dengan Djojosoedarso, Stoneburner (2002:4) memandang manajemen risiko dalam implementasi teknologi informasi diorganisasi merupakan proses yang memungkinkan manajer

teknologi informasi untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem teknologi informasi dan data yang mendukung misi organisasi.

Sedangkan dalam penerapan sistem informasi, secara khusus Gibson (2011:13) mengemukakan "*risk management is the practice of identifying, assessing, controlling, and mitigating risks*". Manajemen risiko diartikan sebagai kegiatan praktis tentang identifikasi, penilaian, pengontrolan, dan peringatan risiko. Pelaksanaan manajemen risiko merupakan tahapan kegiatan organisasi dalam mengidentifikasi dan memandang sumber risiko, kerentanan risiko secara menyeluruh dan terkontrol dengan dilaksanakan evaluasi proses secara berkesinambungan.

Suatu upaya dari perencanaan, pengorganisasian, kepemimpinan, pengendalian sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian dan ketidakpastian terhadap biaya serta konsekuensinya adalah kegiatan manajemen risiko di organisasi secara umum. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri atas beberapa tahapan kegiatan, ketika diterapkan secara benar memungkinkan terjadinya perbaikan terus menerus dalam proses pengambilan keputusan.

Sistem Informasi

Sistem Informasi menurut Oetomo (2002:11) sebagai kumpulan elemen yang saling berhubungan satu dengan yang lain membentuk satu kesatuan untuk mengintegrasikan data, memproses dan menyimpan serta mendistribusikan informasi. Sedangkan Indrajit (2000) mendefinisikan sistem informasi sebagai suatu kumpulan dari komponen-komponen dalam perusahaan atau organisasi yang berhubungan dengan proses penciptaan dan pengaliran informasi. Tantra (2012:2) menyebutkan bahwa sistem informasi merupakan cara yang terorganisir, untuk mengumpulkan, memasukkan, dan memproses data dan menyimpannya, mengelola, mengontrol dan melaporkannya sehingga dapat mendukung perusahaan atau organisasi untuk mencapai tujuan.

Sistem informasi perpustakaan merupakan rangkaian komponen sistem baik mesin atau manusia yang disusun, dirancang untuk memproses data agar informasi dapat tersajikan untuk mendukung fungsi operasional perpustakaan dalam proses pengambilan keputusan. Sistem informasi

perpustakaan dapat mengintegrasikan bidang pekerjaan perpustakaan yang meliputi kegiatan pengadaan, inventarisasi, katalogisasi, sirkulasi bahan pustaka, pengelolaan anggota, statistik dan penelusuran koleksi perpustakaan.

Kerangka Kerja Manajemen Risiko

Dalam melaksanakan kegiatan manajemen risiko teknologi informasi dan sistem informasi terdapat beberapa kerangka kerja yang merupakan kumpulan prosedur standar dalam mengelola dan memberikan pemahaman untuk kegiatan manajemen risiko yang dilaksanakan secara bertahap. NIST mengeluarkan rekomendasi melalui publikasi khusus *framework* NIST SP 800-30 tentang *Risk Management Guide For Information Technology System*.

Terdapat tiga proses dalam manajemen risiko yakni: proses penilaian risiko, proses peringanan (mitigasi) risiko dan proses evaluasi risiko. Masing-masing tahapan proses tersebut memiliki kerangka kerja terstruktur untuk memberikan penjelasan kerangka kerja manajemen risiko teknologi informasi. Proses kerangka kerja NIST meliputi: *risk assessment* (penilaian risiko), *risk mitigation* (peringanan risiko) dan *risk evaluation* (evaluasi risiko)

Jenis-jenis Ancaman Sistem Informasi Perpustakaan

Sumber ancaman yang memungkinkan mengganggu aktivitas layanan sistem informasi perpustakaan antara lain:

a. Ancaman Alam

Ancaman alam dapat dikategorikan sebagai bencana (*hazard*) yang dapat ditimbulkan dari ancaman air seperti banjir, tsunami, intrusi air laut, kelembaban tinggi, badai, pencairan salju.

Ancaman tanah: longsor, gempa bumi, gunung meletus.

Ancaman alam lain: kebakaran hutan, petir, tornado, angin ribut.

b. Ancaman lingkungan/teknis

Ancaman lingkungan meliputi: gangguan listrik seperti putusnya aliran listrik, penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dalam jangka waktu yang lama. Medan elektromagnetik, gangguan pengerat (tikus), efek bahan kimia obat pembunuh serangga, kebocoran AC (*air conditioning*).

c. Ancaman manusia

Ancaman yang berasal dari manusia terbagi menjadi dua ancaman dari intern organisasi perpustakaan dan ekstern organisasi perpustakaan.

Kerangka konsep penelitian ini sesuai dengan pendapat Gibson (2011:13) bahwa manajemen risiko sebagai kegiatan praktis tentang identifikasi, penilaian, pengontrolan, peringanan risiko. Gambaran kegiatan manajemen risiko sistem informasi tersebut, kajian penelitian ini menggunakan *framework* NIST *Special Publication* 800-30 sebagai metodologi terstruktur yang memberikan gambaran tahapan kegiatan manajemen risiko yang dimulai dari kegiatan penilaian risiko, peringanan risiko dan evaluasi pengontrolan risiko.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Penelitian dilakukan dengan teliti, mendalam dan menyeluruh dengan cara melakukan wawancara mendalam dan pengamatan langsung (*observasi*) serta mendeskripsikan hal-hal yang berkaitan dengan obyek penelitian. Kajian utama yang akan diteliti yakni pelaksanaan manajemen risiko sistem informasi perpustakaan dengan menggunakan kerangka kerja manajemen risiko NIST *Special Publication* 800-30 sistem informasi perpustakaan dan mengetahui mengapa Perpustakaan UGM melaksanakan kegiatan manajemen risiko sistem informasi. Pengamatan ditujukan pada manusia/orang yakni pustakawan sebagai operator dan penanggung jawab layanan di Perpustakaan UGM yang memiliki kegiatan dan memiliki situasi sosial dalam menerapkan konsep manajemen risiko sistem informasi perpustakaan. Apabila dilihat dari tujuan penelitian, jenis penelitian ini adalah studi kasus. Secara umum studi kasus merupakan strategi yang lebih cocok bila pokok pertanyaan suatu penelitian berkenaan dengan *how* dan *why*.

Pemilihan Kasus

Penelitian ini merupakan penelitian studi kasus tunggal yang bersifat holistik. Penelitian dilakukan di Perpustakaan UGM pada bulan Januari sampai dengan Februari 2014. Alasan pemilihan tempat penelitian di Perpustakaan UGM karena Perpustakaan UGM telah mengaplikasikan sistem

informasi perpustakaan secara terintegrasi dalam setiap kegiatan layanan kepada pemustaka pada bulan tersebut. Perpustakaan UGM menjadi unit penunjang bagi organisasi induk dalam memberikan layanan informasi dan aset-aset informasi digital yang berkontribusi terhadap hasil pemeringkatan akses *webometric* UGM dan Perpustakaan menempati ranking pertama penilaian di tingkat nasional, namun Perpustakaan UGM belum melaksanakan kegiatan manajemen risiko sistem informasi sebagai prosedur kerja yang harus dilaksanakan sehingga merupakan sesuatu yang menarik untuk diteliti.

Teknik Pengambilan Sampel

Penelitian kualitatif tidak menggunakan istilah populasi dan sampel, tetapi dinamakan situasi sosial yang terdiri atas tiga elemen yaitu tempat, pelaku dan aktivitas yang berinteraksi secara sinergis. Situasi sosial dalam penelitian ini merupakan kesatuan dalam organisasi perpustakaan dengan berbagai aktivitas dari pustakawan yang berinteraksi secara langsung dengan sistem informasi perpustakaan yang berkaitan dengan penerapan manajemen risiko sistem informasi. Penentuan sumber data pada orang yang diwawancarai dilakukan secara purposive, yakni dipilih dengan pertimbangan dan tujuan tertentu.

Informan penelitian adalah petugas perpustakaan yang memiliki pengalaman dan berinteraksi dengan sistem informasi perpustakaan. Informan penelitian dapat dikategorikan sebagai berikut: 1. Kepala Perpustakaan UGM, 2. Kabid *Database* dan Jaringan Perpustakaan UGM, 3. Bagian layanan sirkulasi Perpustakaan UGM, 4. *IT Support System Analysis*, 5. Operator bagian perlengkapan.

Teknik Pengumpulan Data

Teknik pengumpulan data yang sesuai untuk menggali informasi dari informan untuk menjawab pertanyaan penelitian adalah dengan melakukan wawancara mendalam (*indepth interview*) dengan menggunakan panduan wawancara semistruktur (*interview guide*) dan observasi (pengamatan langsung). Pengumpulan data lapangan terlebih dahulu dengan melaksanakan observasi pendahuluan tentang tema kajian yang diteliti untuk lebih mendalami kajian yang akan diteliti. Wawancara dilaksanakan tanpa interupsi, sehingga informan mengutarakan pengalamannya secara mendalam, mendetail dengan terlebih dahulu

mendengarkan pertanyaan wawancara dari peneliti. Apabila ada pengungkapan pendapat yang tidak sesuai dengan tema, maka peneliti memfokuskan pada tema pokok kajian penelitian.

Teknik Analisis Data

Analisis data dalam penelitian bersifat deskriptif analitis. Deskriptif karena hasil dari penelitian diharapkan mampu memberikan gambaran secara sistematis, rinci dan menyeluruh tentang pelaksanaan manajemen risiko sistem informasi perpustakaan di Perpustakaan UGM. Penelitian ini berusaha menggambarkan situasi atau kejadian, sedangkan analitis karena dilakukan analisa untuk menjawab beberapa permasalahan seperti yang telah dirumuskan sebelumnya. Semua data baik berupa jawaban dari informan atas pertanyaan yang diajukan melalui wawancara, ataupun yang diperoleh dari observasi dihimpun menjadi satu. Setelah terkumpul lengkap, data diolah dan dianalisis secara kualitatif yakni memperhatikan fakta yang terjadi dilapangan berdasarkan variabel yang sudah ditentukan, kemudian dimasukkan dalam tahap-tahap analisis. Selanjutnya diambil kesimpulan dengan menggunakan metode deduktif yakni berdasarkan teori yang bersifat umum untuk menjelaskan hubungan data dengan data lainnya.

Teknik Pemeriksaan Data

Teknik pemeriksaan data pada penelitian ini menggunakan metode triangulasi dengan menggabungkan berbagai teknik pengumpulan data dan sumber data yang telah ada. Triangulasi merupakan teknik pengumpulan data yang berbeda-beda untuk mendapatkan data dari sumber yang sama dengan cara observasi, wawancara mendalam dan dokumentasi. Sedangkan triangulasi sumber, peneliti mendapatkan data dari sumber informan yang berbeda-beda dengan teknik yang sama.

HASIL DAN PEMBAHASAN

Proses Penilaian Risiko (*Risk Assessment*)

Tahapan penilaian risiko menggunakan *framework* NIST SP 800-30 meliputi proses sebagai berikut:

Karakteristik sistem

Komponen karakteristik sistem untuk sistem informasi SIPUS meliputi: perangkat keras, perangkat lunak, peralatan jaringan, data dan informasi, serta operator. Perangkat keras untuk *client* menggunakan personal komputer dengan

perangkat lunak *windows xp*, *windows 7* dan *windows 8*. Untuk *server* menggunakan *apache server*, *mysql*, pemrograman *php* yang secara umum menggunakan *virtual server* yang ditempatkan di PSDI UGM. Operator terbagi menjadi operator untuk pustakawan dan untuk administrator sistem. Klasifikasi data dan informasi meliputi data masukan dari SIPUS, data statistik, data transaksi, dan data koleksi.

Identifikasi ancaman

Berdasarkan hasil wawancara dan observasi lapangan, identifikasi ancaman yang mengganggu sistem informasi meliputi ancaman listrik padam, ketergantungan pada kemampuan *server* sistem informasi untuk *backup server hang* yang mengalami kerusakan dan ketergantungan pustakawan pada *IT support* meskipun kesadaran, pengetahuan dan pengalaman pustakawan sudah dimiliki oleh setiap individu.

Identifikasi kerentanan

Kerentanan yang teridentifikasi meliputi keamanan (*security*) sistem yang di *publish* menggunakan *internet*, penggunaan *password* sistem informasi secara bersama-sama, otorisasi hak akses yang berkaitan dengan data sensitif sistem informasi perpustakaan.

Analisa kontrol

Analisa kontrol secara khusus untuk kegiatan penilaian risiko belum terdokumentasi, tetapi hanya berdasarkan pada pengetahuan dan kesadaran dari pustakawan dalam mengenali, mendeteksi dan melaksanakan tindakan pencegahan terhadap risiko yang mengancam. Berdasarkan hasil observasi analisa kontrol yang memungkinkan dapat digunakan untuk penilaian risiko meliputi: 1. Aturan dan tanggung jawab keamanan teknologi informasi. 2. Sosialisasi dan perencanaan operasional tentang sistem informasi. 3. Klasifikasi data sensitif. 4.

Perencanaan perbaikan bencana aset TI. 5. Manajemen *backup*. 6. Manajemen *password*. 7. Ekskripsi sistem. 8. Fasilitas keamanan lingkungan. 9. Lisensi *software*, 10. Kontrol otorisasi hak akses. 11. Manajemen *account*, 12. Proteksi ancaman virus. Berdasarkan analisa kontrol yang telah disebutkan, maka potensi ancaman yang dapat dieksploitasi menjadi sumber risiko meliputi: 1. Listrik, 2. *Password*. 3. Otorisasi hak akses, 4. Keamanan sistem. 5. Sumber daya manusia. 6. *Backup server hang*.

Kemungkinan yang menentukan

Hasil kemungkinan risiko yang mengancam sistem informasi dapat dideskripsikan menggunakan kemungkinan ancaman risiko dengan menganalisa analisa kontrol yang dilaksanakan untuk mengantisipasi potensi ancaman risiko. Ancaman risiko berjalan efektif atau bahkan analisa kontrol tidak dapat mencegah potensi ancaman risiko yang mengganggu sistem informasi. Hasil dari analisa dalam proses ini adalah tinggi apabila kemungkinan risiko yang menentukan dan analisa kontrol tidak bisa secara efektif mengantisipasi sumber ancaman risiko. Bernilai sedang apabila kontrol analisa yang diterapkan mampu mengantisipasi dan menurunkan risiko, sedangkan rendah apabila efektivitas analisa risiko dapat mengantisipasi sumber risiko yang mengancam dapat berjalan dengan baik.

Hasil dari kemungkinan risiko yang menentukan dapat diidentifikasi listrik memiliki kemungkinan risiko tinggi, *password* kemungkinan risiko tinggi, otorisasi hak akses kemungkinan risiko sedang, *backup server hang* risiko tinggi, keamanan sistem memiliki kemungkinan risiko tinggi dan sumber daya manusia dengan kemungkinan risiko rendah.

Analisa dampak

Berdasarkan kemungkinan risiko yang mengancam, maka dampak dari risiko tersebut dapat dilihat dalam tabel 1.

Tabel 1. Dampak Risiko

Jenis Risiko	Konsekuensi	Nilai Dampak
Listrik	<ul style="list-style-type: none"> Terhentinya proses pengambilan keputusan dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan. Terhentinya layanan informasi perpustakaan dan menurunnya kemampuan sistem yang berakibat pada kegagalan penilaian aset informasi yang dilayangkan. 	Tinggi
Password	<ul style="list-style-type: none"> Hilangnya kemampuan sistem dalam mengantisipasi berbagai sumber ancaman. Menambah jumlah <i>history log</i> sistem yang menurunkan kecepatan sistem, sistem menjadi lambat. 	Tinggi
Otorisasi Hak Akses	<ul style="list-style-type: none"> Hilangnya kemampuan perlindungan informasi karena hak akses yang terbuka. Manipulasi data sensitif yang dimiliki oleh perpustakaan 	Sedang
Backup Server Hang	<ul style="list-style-type: none"> Hilangnya reputasi perpustakaan sebagai penyedia informasi. Hilangnya kemampuan perlindungan terhadap aset informasi. 	Tinggi
Keamanan Sistem	<ul style="list-style-type: none"> Masuknya berbagai <i>virus</i> ke sistem informasi dan manipulasi data sensitif. Kemampuan perlindungan menjadi terganggu. 	Tinggi
Sumber Daya Manusia	<ul style="list-style-type: none"> Ketergantungan pada 1 personil. Antisipasi ancaman yang tidak terdeteksi karena keterbatasan kemampuan SDM. 	Sedang

Risiko yang menentukan

Berdasarkan hasil analisis diperoleh risiko yang menentukan seperti yang digambarkan dalam tabel 2

Tabel 2. Penentuan Risiko

Tipe Risiko	Skor Kemungkinan Ancaman	Skor Dampak	Skor Risiko	Predikat Level Rangking
Backup server hang	1.0(tinggi)	100 (tinggi)	100	Tinggi
Listrik	1.0(tinggi)	100 (tinggi)	100	Tinggi
Keamanan sistem	1.0(tinggi)	100 (tinggi)	100	Tinggi
Password	1.0(tinggi)	100 (tinggi)	100	Tinggi
Otorisasi hak akses	0.5(sedang)	50 (sedang)	25	Sedang
Sumber Daya Manusia	0.5(sedang)	50 (sedang)	25	Sedang

Dokumentasi hasil

Dokumentasi hasil penilaian risiko berupa profil risiko yang mengancam sistem informasi dan solusi pencegahan melalui rekomendasi kontrol sebagai tindakan proses berikutnya melalui kegiatan mitigasi risiko

Tabel 3. Rekomendasi kontrol

No	Tipe Risiko	Level Risiko	Rekomendasi
1.	<i>Backup Server Hang</i>	Tinggi	<ul style="list-style-type: none"> • Penyediaan <i>recovery backup RAID</i>. • <i>Backup</i> secara periodik. • Pemindahan <i>server</i>. • <i>Cloud computing</i> dan Pembuatan <i>dummy server</i>.
2.	Listrik	Tinggi	<ul style="list-style-type: none"> • Perbaikan dan penambahan kapasitas genzet. • Pembelian dan penggunaan UPS (<i>uninterrupted power supply</i>)
3.	Keamanan Sistem	Tinggi	<ul style="list-style-type: none"> • Instalasi <i>firewall</i>, antivirus, <i>deep freeze</i> dan • Modifikasi <i>default security system</i>.
4.	<i>Password</i>	Tinggi	<ul style="list-style-type: none"> • Perubahan <i>password</i> secara berkala. • Kerahasiaan <i>password</i>. • Pengaturan <i>password</i> sesuai tupoksi.
5.	Otorisasi Hak Akses	Sedang	<ul style="list-style-type: none"> • <i>Up date</i> dan perubahan hak akses secara periodik.
6.	Sumber Daya Manusia	Sedang	<ul style="list-style-type: none"> • Pelatihan sumber daya manusia. • Penambahan pegawai dan <i>sharing</i> pengetahuan.

Tabel 3 merupakan rekomendasi kontrol yang dapat digunakan sebagai langkah mitigasi risiko pada tahap berikutnya dan disesuaikan dengan visi dan misi Perpustakaan UGM.

Proses Peringatan Risiko (*Risk Mitigation*)

Tahap berikutnya adalah mitigasi risiko berupa tindakan peringatan profil risiko yang sudah terdokumentasi. Setelah dianalisis pada tahap penilaian risiko maka didapatkan profil risiko dengan berbagai proses rekomendasi pemecahan yang sekiranya dapat digunakan dalam proses peringatan risiko yang sesuai dengan kebutuhan di Perpustakaan UGM. Dalam kegiatan mitigasi risiko diperlukan tahapan proses yang meliputi berbagai kegiatan secara bertahap dan berkelanjutan sebagai berikut:

1) Prioritas Aksi

Proses peringatan risiko dimulai dengan mengambil tindakan aksi yang mengacu pada hasil akhir penilaian profil risiko yang terdiri dari risiko *backup server hang*, listrik, *password*, keamanan sistem, otorisasi hak akses

dan sumber daya manusia. Perpustakaan memandang bahwa mitigasi risiko dengan cara memindahkan *server* perpustakaan ke PSDI merupakan bentuk opsi kegiatan yang tepat. Karena adanya jaminan dari lembaga yang memang memiliki kompetensi, serta didukung oleh kebijakan universitas agar semua sistem informasi terintegrasi dalam pengawasan PSDI. Stoneburner (2002) memberikan definisi tentang mitigasi risiko adalah metodologi sistematis yang digunakan oleh manajer senior untuk mengurangi misi risiko.

Prioritas aksi tentang mitigasi risiko yang diambil oleh Perpustakaan UGM yang berhubungan dengan kondisi *server* secara langsung berdampak pada level risiko yang teridentifikasi sebelumnya yakni listrik, password, otorisasi hak akses, keamanan sistem dan sumber daya manusia. Level profil risiko tersebut dapat dikurangi dengan menggunakan kontrol hasil rekomendasi yang sudah dinilai pada tahap sebelumnya.

2) Opsi Evaluasi Rekomendasi Kontrol

Berdasarkan hasil analisis evaluasi kontrol

mitigasi risiko yang telah dilaksanakan di Perpustakaan UGM terungkap bahwa pengembangan dummy server untuk mengantisipasi penggunaan dan akses sistem informasi perpustakaan seluruh UGM secara terintegrasi belum dapat dilaksanakan.

3) Aturan Analisa Akibat dan Biaya

Pada tahap ini kegiatan mitigasi risiko menyesuaikan dengan biaya dan keuntungan dalam upaya untuk meminimalisasi risiko yang teridentifikasi dan hasil rekomendasi yang akan dilaksanakan. Kegiatan analisa biaya dan akibat yang ditimbulkan menjadi perhatian khusus Perpustakaan UGM karena penggunaan biaya harus sesuai dan memiliki tanggung jawab.

Anggaran khusus tentang pelaksanaan manajemen risiko di Perpustakaan UGM belum dialokasikan secara khusus, tetapi untuk risiko ataupun kejadian yang bersifat insidental perpustakaan masih dapat menganggarkan karena menyangkut layanan kepada pemustaka yang tidak boleh dihentikan. Sebagai hasil analisis antisipasi yang berkaitan dengan sistem informasi perpustakaan, Perpustakaan UGM menempatkan staf khusus programmer sebagai supportingsystem dari PSDI dengan kebijakan dan anggaran khusus.

4) Pemilihan Kontrol

Pemilihan kontrol yang dilaksanakan oleh Perpustakaan UGM adalah dengan memindahkan risiko (*Risk Transfer*) ke lembaga universitas yang memiliki kemampuan dan kompetensi dalam perawatan sistem informasi. Proses pemindahan risiko tersebut dilakukan dengan memindahkan *server* Perpustakaan UGM beserta sumber data ke *server* PSDI. Perpustakaan UGM dapat mengakses *server* sistem informasi melalui jaringan internet. PSDI merupakan lembaga di UGM yang memiliki wewenang dalam menunjang penggunaan teknologi informasi dan aset-aset informasi yang ada di seluruh UGM.

5) Tugas dan Tanggung Jawab

Mitigasi risiko sebagai proses kegiatan yang berkelanjutan dan terus menerus memerlukan peran dari personil yang bertanggung jawab dan memiliki pengetahuan dalam bidang teknologi informasi. Secara struktur organisasi, Perpustakaan UGM memiliki bidang database dan jaringan yang bertanggung jawab mengelola sistem informasi dan objek-objek informasi digital.

Secara personil penanggungjawab *database* dan jaringan merupakan pustakawan yang memiliki pemahaman dan pengetahuan dalam bidang teknologi informasi dan memiliki kemampuan manajerial sebagai seorang penanggung jawab teknologi informasi. Tugas dan tanggung jawab untuk kegiatan mitigasi risiko dilaksanakan oleh kaid *database* dan jaringan dibantu oleh *IT support system*.

6) Pengembangan Rencana Perlindungan

Pengembangan rencana perlindungan sesuai dengan rekomendasi kontrol pada tahap penilaian risiko. Rekomendasi kontrol tersebut sebagai acuan rencana perlindungan aset informasi di Perpustakaan UGM.

7) Implementasi Kontrol

Pada tahap ini Perpustakaan UGM telah mengimplementasikan proses mitigasi risiko dengan kegiatan pemindahan risiko (*risk transfer*) pada profil risiko yang sudah teridentifikasi yakni risiko *backup server* yang memiliki level risiko tinggi. Pemindahan server sistem informasi perpustakaan ke pihak PSDI sebagai solusi yang tepat mengantisipasi sumber ancaman yang dapat mengakibatkan terganggunya layanan sistem informasi perpustakaan. Profil sumber risiko yang lain seperti listrik, *password*, otorisasi hak akses, keamanan sistem dan sumber daya manusia, Perpustakaan UGM berupaya menghilangkan sumber risiko tersebut dengan berbagai kegiatan dan memperhatikan rekomendasi kontrol yang telah dilaksanakan.

Evaluasi Risiko (*Risk Evaluation*)

Evaluasi risiko merupakan tahap akhir dalam proses manajemen risiko sistem informasi perpustakaan dengan menggunakan *framework* NIST *Special Publication* 800-30. Perpustakaan UGM melaksanakan kegiatan evaluasi secara periodik sesuai dengan kebutuhan dan solusi pemecahan berdasarkan kasus yang ditangani, termasuk juga dalam memandang manajemen risiko sebagai bagian dari perpustakaan untuk selalu dilaksanakan kegiatan evaluasi secara terus menerus.

Backup data dan aplikasi sistem informasi menjadi kegiatan rutin yang dilaksanakan secara periodik dan penambahan fitur-fitur baru untuk kehandalan sistem informasi menjadi bagian dari evaluasi dalam kegiatan manajemen risiko di Perpustakaan UGM.

Faktor-faktor yang Mempengaruhi Pelaksanaan Manajemen Risiko

Pelaksanaan manajemen risiko sistem informasi perpustakaan di Perpustakaan UGM telah dilaksanakan meskipun tidak secara khusus dalam satu kegiatan secara prosedur sesuai dengan kerangka kerja manajemen risiko dalam menilai, meminimalisasi dan mengevaluasi risiko yang mengancam sistem informasi. Pemahaman pustakawan UGM akan proses manajemen risiko hanya bersifat "insidental" yang saat itu terjadi dan segera dilakukan tindakan perbaikan secepatnya tanpa merencanakan kegiatan antisipasi dan tindakan deteksi ancaman risiko yang sewaktu-waktu dapat mengganggu sistem informasi perpustakaan.

Kegiatan yang dilaksanakan oleh perpustakaan UGM dalam proses manajemen risiko merupakan mandat dari universitas dan persepsi pimpinan perpustakaan tentang bidang kerja dan kewenangan yang berkaitan dengan penggunaan teknologi informasi dan sistem informasi merupakan "urusan" PSDI menjadi salah satu faktor yang menyebabkan Perpustakaan UGM belum maksimal dalam menilai berbagai macam sumber ancaman risiko yang akan mengganggu sistem informasi perpustakaan. Proses mitigasi atau peringanan risiko sebagai upaya untuk meminimalisasi akibat risiko yang mengancam, hanya sebatas pengetahuan backup data yang dilaksanakan secara periodik yang dilaksanakan oleh *IT support*. Tindakan pencegahan dan deteksi ancaman risiko dengan melaksanakan kegiatan mitigasi risiko dengan cara memindahkan (*transfer*) risiko server sistem informasi perpustakaan ke PSDI, secara garis besar sebagai upaya untuk memudahkan pengawasan lembaga induk UGM dalam satu wadah melalui sistem informasi terpusat. Kegiatan manajemen risiko hanya yang bersifat saat itu terjadi yang terkait dengan layanan informasi perpustakaan untuk memberikan layanan maksimal kepada pemustaka apabila terjadi gangguan terhadap sistem informasi perpustakaan.

Kebijakan pimpinan lembaga induk dan persepsi Kepala Perpustakaan UGM tentang pelaksanaan manajemen risiko sistem informasi perpustakaan menjadi faktor yang mempengaruhi mengapa Perpustakaan UGM belum melaksanakan kegiatan manajemen risiko sesuai dengan kerangka kerja yang dilaksanakan dalam lingkup organisasi perpustakaan itu sendiri. Hal ini dilatarbelakangi oleh penerapan teknologi web sistem informasi perpustakaan dan karakteristik Perpustakaan UGM yang layak disebut sebagai perpustakaan modern

dengan aplikasi teknologi informasi secara terintegrasi.

Faktor lain yang mempengaruhi pelaksanaan manajemen risiko sistem informasi perpustakaan di Perpustakaan UGM adalah keterbatasan kemampuan sumber daya manusia yang meliputi kemampuan pustakawan dan operator pendukung yang memiliki pengetahuan terkait dengan teknologi *web* dan teknologi informasi secara umum.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilaksanakan maka diperoleh kesimpulan berikut:

- a. Proses penilaian risiko (*risk assessment*) mendeskripsikan profil risiko yang mengancam sistem informasi perpustakaan berdasarkan ranking level risiko meliputi jenis risiko teknis dan risiko manusia. Risiko teknis terdiri dari *backup server hang* dengan level risiko tinggi, listrik level risiko tinggi, keamanan (*security*) sistem dengan level risiko tinggi, *password* dengan level risiko tinggi, dan otorisasi hak akses dengan level risiko sedang. Jenis risiko manusia teridentifikasi profil risiko dengan ranking sedang. Perpustakaan UGM belum memiliki dokumentasi penilaian risiko sebagai standar kegiatan dalam proses penanganan sumber ancaman yang menghambat sistem informasi perpustakaan. Penilaian risiko hanya berdasarkan kejadian yang bersifat "insidental" yang diantisipasi dengan memaksimalkan peran *IT support* dan kesadaran dari pustakawan dalam mengantisipasi berbagai ancaman risiko sistem informasi.
- b. Mitigasi risiko atau peringanan risiko di Perpustakaan UGM dilaksanakan dengan cara memindahkan risiko yakni dengan memindahkan server sistem informasi perpustakaan ke PSDI sebagai lembaga yang berwenang dan memiliki kompetensi dalam merawat aset sistem informasi di lingkungan UGM. Pemindahan risiko ke PSDI terkait dengan kebijakan lembaga induk yang memfasilitasi pengelolaan sistem informasi dalam satu wadah sebagai upaya untuk memudahkan pengawasan. Persepsi dari pimpinan perpustakaan tentang kemampuan sumber daya manusia yang masih terbatas dan delegasi kewenangan bidang teknologi informasi bukan kewenangan bagi perpustakaan menyebabkan pimpinan perpustakaan mengambil kebijakan mentransfer risiko kepada lembaga yang memiliki

kompetensi, disamping adanya jaminan perawatan untuk kelangsungan sistem informasi perpustakaan.

- c. Evaluasi kegiatan manajemen risiko belum dilaksanakan sesuai dengan prosedur, hanya dilaksanakan dengan kegiatan *backup* data secara periodik dan konsistensi dari pustakawan untuk selalu mengantisipasi berbagai macam kejadian yang dapat mengancam sistem informasi perpustakaan.
- d. Kerangka kerja NIST *Special Publication* 800-30 mampu mendeskripsikan profil ancaman risiko yang mengganggu pengembangan perpustakaan berbasis teknologi *web* dan memberikan solusi mitigasi risiko sebagai tindakan peringatan risiko, serta memiliki metode pengawasan secara menyeluruh melalui evaluasi pelaksanaan manajemen risiko sistem informasi perpustakaan dalam siklus hidup pengembangan sistem informasi.

Berdasarkan beberapa kesimpulan di atas, saran rekomendasi yang bermanfaat untuk digunakan dalam kegiatan manajemen risiko sistem informasi di Perpustakaan UGM, sebagai berikut:

- a. Perlunya pembuatan dokumentasi penilaian risiko, mitigasi risiko dan evaluasi risiko untuk mengantisipasi berbagai ancaman risiko yang memberikan dampak negatif bagi Perpustakaan UGM. Dokumentasi manajemen risiko diperlukan sebagai acuan mengantisipasi risiko dengan makin banyaknya aset informasi yang dimiliki oleh Perpustakaan UGM yang mengalami ketidakpastian.
- b. Pemahaman pustakawan akan risiko yang mengancam sistem informasi tidak hanya berkaitan dengan *server* dan backup data saja, tetapi memerlukan pemahaman teknis lain dalam bidang IT yang memerlukan sosialisasi dari pengambil kebijakan. Pemahaman akan tindakan deteksi ancaman dan tindakan pencegahan dapat dilaksanakan oleh pustakawan sehingga tidak tergantung pada *IT support*.
- c. Diperlukan penelitian lanjutan yang lebih spesifik tentang manajemen risiko sistem keamanan, perilaku pustakawan dalam mengantisipasi ancaman risiko dan pengembangan perpustakaan berbasis *cloud computing* untuk mengkaji aset kritis sistem informasi yang berkaitan dengan teknologi *web* 2.0 yang memiliki tingkat ancaman risiko yang

lebih besar dengan kemampuan pemahaman teknologi informasi yang lebih mendalam.

DAFTAR PUSTAKA

- Darmawi, Herman. *Manajemen Risiko*. Jakarta: Bumi Aksara, 2006.
- Djojosoeharso, Soeisno. *Prinsip-prinsip Manajemen Risiko dan Asuransi*. Jakarta: Salemba Empat, 1999.
- Gibson, Darril. *Managing Risk in Information Systems*. Sudbury: Jones&Bartlett Learning, 2011.
- Hanafi, Mamduh M. *Manajemen Risiko*. Yogyakarta: UUPSTIMYKPN, 2009.
- Idroes, Ferry N. *Manajemen Risiko Perbankan: Pemahaman Pendekatan 3 Pilar Kesepakatan Basel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesia*. Jakarta: Rajawali Pers, 2008.
- Indrajit, Richardus Eko. *Pengantar Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi*. Jakarta: Elex Media Komputindo, 2000.
- Maulana, M.M dan Supangkat, S.H. "Pemodelan Framework Manajemen Risiko Teknologi Informasi untuk Perusahaan di Negara Berkembang". Pada Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia. 121-126. 3-4 Mei, Bandung, 2006.
- Muntashir. *Analisis Webometrics pada Perpustakaan Perguruan Tinggi Negeri di Indonesia*. Visi Pustaka. Vol.14. No.2., Agustus, 2012.
- Oetomo, Budi Sutedjo Dharma. *Perencanaan dan Pembangunan Sistem Informasi*. Yogyakarta: Penerbit Andi, 2002.
- Pinontoan, Jimmy H. *Manajemen Risiko TI – Konsep-konsep*. Majalah PC Media. Oktober 2010.
- _____. *Manajemen Risiko TI – Penerapan Praktis*. Majalah PC Media. November 2010.
- Undang-Undang Nomor 43 Tahun 2007 tentang Perpustakaan.
- Setiarso, Bambang. *Penerapan Teknologi Informasi dalam Sistem Dokumentasi dan Perpustakaan*. Jakarta: Grasindo, 1997.

Suduc, A.M., M. Bizoi dan F.G. Filip, *Audit for Information Systems Security*. Journal Informatica Economica, 14(1), 43-48. 2010.

Supriyanto, Wahyu dan Ahmad Muhsin. *Teknologi Informasi Perpustakaan; Strategi Perencanaan Perpustakaan Digital*. Yogyakarta: Kanisius. 2008.

Stoneburner G, A. Goguen and A. Feringa. *Risk Management Guide for Information Technology Systems.*, Recommendation of the National Institute of Standart and Technology Special Publication 800-30. 2002.

Tantra, Rudy. *Manajemen Proyek Sistem Informasi*. Yogyakarta: Penerbit Andi. 2012.