



Analisis Penerapan Risk Management Terhadap Sistem Informasi Management Perbankan

Zulhasby Assdqy Nasution¹, Muhammad Irwan Padli Nasution², Sri Suci Ayu Sundari³

^{1,2,3} Universitas Islam Negeri Sumatera Utara

Corresponding Author : ✉ zulhasbynasution@gmail.com

ABSTRACT

The purpose of this study is to analyze risk management in management information systems. Therefore, banks and companies are advised to carry out detailed identification by looking at the hazards and risks at each stage of operation, the banking management information system workforce. The author also provides risk advice to banking institutions so that they use management in management information systems carefully and continue to pay attention and rediscover the usefulness of the risk management they use, besides that the most important thing is the development of risk management on management information systems, so as to protect all existing data on the information system. An institution or an organization that utilizes information technology to support ongoing information system activities, where the success of the services of these institutions refers to the extent to which information technology management has been implemented. The results that will be obtained from this risk management are that it will be seen that sources of threats can pose a threat to the management information system, such as human threats (hackers/crackers and insiders), as well as threats of natural disasters (floods, earthquakes, fires and others).). The rapid development of information technology at this time requires every institution or company to always develop in all its fields, with the existence of information technology now companies can apply it as well as possible. On the other hand, the application of information technology requires investment costs that are quite expensive and can pose a significant risk of failure. When a company situation like this requires strong consistency in managing and implementing information systems. Therefore, risk management is needed by a company so that it can find out what risks can occur if implementing risk management on the banking management information system. The COBIT 4.1 framework is one of the frameworks that is often used and is very suitable for the needs of institutions and banks, because the COBIT 4.1 framework is certain to have aligned information systems with business processes, information technology resources, identified risks, carried out a risk assessment, managing risks appropriately, and being able to produce recommendations in order to achieve the desired targets.

Keywords

Management Risk, Management Information System



This work is licensed under a
[Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

PENDAHULUAN

Pada tahun 2010, terdapat kurang lebih dari 200 bank yang ada di dunia bersiap siap perubahan jangka panjang yaitu inisiatif untuk mengadopsi *Information and Tehnology (IT)*. Dari beberapa bank tersebut, 46 nya berada di Asia Pasifik 1 pada saat itu mereka meyakini bahwa 10 tahun ke depan, perbankan akan ikut pada perubahan yang tidak di sangka - sangka sebelumnya, dan perbankan akan menghadapi risiko risiko baru yang sama sekali belum pernah terjadi. Perkembangan tehnologi informasi di era ini semakin canggih, sehingga membawa kegiatan dan aktifitas manusia dunia memasuki era baru, yaitu era yang sering disebut - sebut sebagai era revolusi industri 4.0. Era yang baru ini dilihat dari perkembangan berbagai inovasi - inovasi tehnologi seperti Internet of Things (IoT), Cloud Computing, Artificial Intelligence(AI), Syber Security, Additive Manufacturing, System Integration dan yang terakhir Machine Learning. Ditahun 2020, ketika berbagai macam sektor ekonomi dan bisnis tidak dapat beraktivitas dikarenakan adanya pandemi COVID-19, khalayak perbankan berpendapat bahwa pada tahun 2025 atau 5 tahun ke depan, fungsi risiko di bank kemungkinan besar akan berbeda secara nyata dari sebelum - sebelumnya. Sebab, telah diprediksi bahwa pada tahun 2025 lebih daris 1/2 jiwa di dunia ini dan juga termasuk dibagian Asia Tenggara akan beralih ke neobanks atau bank digital. Oleh karena itu pihak perbankan wajib melangkah lebih cepat untuk mengadopsi tehnologi digital, agar perbankan dapat segera berevolusi menjadi bank digital dengan jumlah risiko yang sedikit.

Memantau serta mempertimbangkan sebuah risiko merupakan suatu proses dimana system informasi management perusahaan, baik dalam perbankan maupun perusahaan perusahaan lainnya memantau seluruh resiko untuk terhindar dari risiko yang lebih besar. Adapun alasan utama mengapa pentingnya menerapkan management risk terhadap system informasi management dikarenakan untuk menerapkan visi misi serta perlindungan asset perusahaan yang kerap mengalami kemunculan risiko risiko baru.

Dalam penggunaan sistem informasi akan muncul berbagai risiko yang dapat mengganggu kegiatan sistem informasi yang tengah berlangsung, sehingga akibatnya terjadi kerugian pada lembaga lembaga managemen perbankan . Risiko yang kerap muncul pada sistem informasi perlu diatasi, agar masalah - masalah yang ditimbulkan tidak sampai mengakibatkan penggunaan tehnologi informasi terhambat kinerjanya yang dapat mengakibatkan kerugian lembaga lembaga keuangan, baik materi maupun diluar materi. Sehingga manajemen Risk terhadap sistem informasi sangat dan dibutuhkan di lembaga - lembaga perbankan. NIST SP 800-30 merupakan kerangka kerja yang kerap digunakan dalam manajemen risiko sistem informasi, yaitu ada 3 tahapan yang terdapat

dalam proses manajemen risiko, yaitu Risk Identification, Risk assessment (Penilaian risiko), dan Risk Treatment.

METODE PENELITIAN

Dilakukan agar dapat mengetahui bagaimana menerapkan manajemen risiko dalam system informasi management, sehingga dapat meminimalisir risiko yang muncul pada perusahaan dan juga risiko operasional pelayanan system informasi manajemen yang ada, baik itu manfaat yang diperoleh apabila menerapkan risk management tersebut. Adapun metode penelitian yang saya gunakan yaitu metode kualitatif, dikarenakan penelitian dilakukan dengan situasi yang natural dan mengutamakan data dari bukti fenomena yang terjadi. Dan penelitian ini akan dilakukan menggunakan pendekatan kualitatif dengan metode study kasus dan metode evaluative.

HASIL DAN PEMBAHASAN

Dari hasil penelitian yang dilakukan berdasarkan analisis study kasus dan metode evaluative, dapat dihasilkan bahwa penerapan risk management terhadap system informasi management merupakan system yang harus dimiliki oleh setiap perusahaan dan dikembangkan, sehingga kemunculan risiko yang ada akan semakin sedikit. Beberapa risiko yang mungkin sering terjadi di dalam system informasi management suatu perusahaan yaitu virus yang menyerang system informasi, sehingga dapat menjadikan kinerja yang ada terganggu. Dan juga serangan para hacker yang dapat mengacaukan system, bahkan sampai mencuri data yang telah dirahasiakan oleh perusahaan. Hal seperti risiko yang telah dijelaskan di atas membuktikan bahwa Risk management sangatlah penting dan harus dimiliki oleh system informasi manajemen. Risiko system informasi juga dapat mempengaruhi operasional suatu perusahaan dan juga dapat menimbulkan tantangan baru ketika hendak mencapai suatu tujuan. Risiko system informasi terbagi menjadi 3 kategori sebagai berikut (IS ACA, 2009) : a) Value enablement risk - hal ini berkaitan dengan kesempatan perusahaan yang hilang dalam penggunaan system informasi untuk meningkatkan efisiensi dan efektifitas/ sebagai enabler inisiatif yang baru, b) Programme and project delivery risk - bagian ini berkaitan dengan teknologi informasi yang berkontribusi terhadap solusi dalam memprogram suatu proyek, c) IT Operation and service delivery risk - hal ini terkait dengan aspek aspek yang kinerja system dan layanan system informasinya dapat merusak nilai perusahaan.

Pengertian Risiko

Definisi risk yang terdapat pada The Oxford English dictionary yaitu 'A chance or possibility of danger, loss, injury, or other adverse consequences'. Riisk atau berisiko memiliki definisi lain dari sumber yang sama 'exposed to danger. Dalam pembahasan ini kata risiko selalu memiliki kaitan dengan sebuah akibat yang akan muncul atau konsekuensi negatif, akan tetapi menghadapi atau mengambil risiko yang ada juga dapat membuahkan dampak positif. Probabilitasnya risiko bisa berujung pada akibat yang tidak dapat dipastikan. Sedangkan risiko menurut ISO Guide 73 ISO 31000 adalah pengaruh ketidakpastian pada tujuan. Pengaruh yang ditimbulkan bisa positif, negatif, atau penyimpangan yang tidak diduga sebelumnya. Risiko juga sering diilustrasikan sebagai sebuah peristiwa, perubahan dalam situasi atau akibat yang akan terjadi. Menurut Institute of Risk Management (IRM) risiko merupakan gabungan antara kemungkinan sebuah kejadian beserta konsekuensinya. Akibatnya beralih dari akibat positif yang akan datang hingga akibat negatif yang akan datang. "Orange Book" dari HM Treasury mendefinisikan risiko sebagai ketidakpastian hasil, dalam berbabagi paparan, timbul dari kombinasi antara dampak dan kemungkinan dari peristiwa. Institute of Internal Auditors menjelaskan bahwa risiko adalah ketidakpastian suatu peristiwa yang terjadi yang berdampak pada pencapaian sebuah tujuan.

Proses manajemen risiko

Manajemen risiko memiliki proses yang berfungsi membantu sistem informasi manajemen dalam melakukan pengambilan hasil keputusan yang lebih baik serta meningkatkan nilai guna maksimum. Meski ada banyak cara dalam mengilustrasikan proses manajemen risiko, langkah-langkah dasar yang ada dalam proses ini hampir sama dan biasanya melingkupi tiga langkah utama yaitu: risk Identification (identifikasi resiko), risk assessment (penilaian suatu risiko), dan risk treatment (modifikasi resiko). Risk identification merupakan sebuah proses dalam memastikan apa, bagaimana, dan mengapa suatu keadaan atau kejadian dapat terjadi. Proses identifikasi risiko harus dibuat secara menyeluruh, harus tersusun berdasarkan faktor-faktor utama agar risiko dapat dinilai secara teratur. Risiko dapat dikenalkan melalui beberapa metode yaitu; checklist, interview atau focused group discussion dan questionnaires. Adapun checklist digunakan agar proses idenntifikasi risiko dilakukan secara sederhana. Checklist juga disusun agar menghindari atau mengurangi sebuah risiko, checklist adalah bagian dari kaidah dokumentasi dan jaminan kualitas organisasi. Adapun pengertian Risk assesment ialah keutuhan proses dari risk analisis dan risk evaluation. Risk analysis merupakan proses yang teratur secara sistem dalam menggunakan sistem informasi yang ada sebagai penentu

seberapa sering risiko muncul dan seberapa besar dampak yang dihasilkan jika risiko tersebut terjadi pada sistem informasi. Proses penilaian risiko pada Risk analysis dapat dilaksanakan menggunakan metode metode yang ada seperti; Bowtie analysis, qualitative analysis atau analisis kualitatif, dan semi quantitative analysis. Sedangkan risk evaluation merupakan sebuah proses yang dilakukan agar dapat membandingkan resiko yang sudah diprediksi dengan perbandingan risiko yang telah ditentukan. Risk treatment memiliki tujuan agar dapat menentukan tindakan yang dilakukan dalam menangani risiko yang telah terdeteksi, supaya mengurangi pengaruh risiko secara keseluruhan. Risk treatment dapat merubah analisis sebelumnya, risk identification (Identifikasi resiko), risk assessment, menjadi tindakan utama untuk mengurangi risiko.

Risk Management Framework

Secara umum telah disetujui bahwa management framework (kerangka kerja manajemen risiko) ialah sebuah dokumen yang memberikan informasi pada proses manajemen risiko. Dalam banyak bentuk kerja manajemen risiko, kegiatan manajemen risiko harus dibuat dalam bentuk lingkungan bisnis, organisasi dan risiko yang kerap dihadapi oleh lembaga lembaga perbankan, Supaya konteks dapat dijelaskan dan didefinisikan, kerangka kerja dibutuhkan dalam mendukung pelaksanaan prosesnya. Berikut ini ialah risk management framework yang dipakai dalam penelitian:

1. Symantec - Risiko manajemen Report Teknologi Informasi (TI) secara menyeluruh dan mendalam telah menjalin hubungan dengan operasi bisnis, risiko yang ada pada TI sendiri pun telah berkembang menjadi bagian dari keseluruhan bagian operasional. Security Risk atau risiko keamanan informasi: keamanan informasi dapat dirubah, diakses atau dipakai oleh orang yang tidak bertanggung jawab. Availability Risk atau risiko ketersediaan; resiko informasi atau aplikasi tidak dapat disalurkan karena system failure (mengalami kegagalan sistem) atau bencana alam, termasuk masa rehabilitas (recovery). Performance Risk atau risiko kinerja; merupakan kinerja yang kurang dari sistem, application, personil atau TI secara menyeluruh, dapat meminimalisir daya produksi atau nilai bisnis.
2. Software COBIT 5 for Risk merupakan sebuah kerangka kerja (framework) yang diciptakan oleh ISACA kepada manajemen teknologi informasi dan manajemen IT. Cobit merupakan toolset (set alat) yang mengharuskan penggunaannya agar menyebrangi perbedaan atau ketidakseimbangan antara kebutuhan kontrol, masalah teknis dan risiko sistem informasi manajemen yang diidentifikasi dalam Cobit dapat diterangkan secara singkat sebagai berikut;

- a. Application atau aplikasi , adalah suatu jalan atau Tool yang digunakan sebagai alat mengolah dan menyimpulkan (meringkas), baik tatacara manual maupun yang terprogram.
- b. Information atau informasi, merupakan Sampel yang sudah jadi untuk keperluan manajemen dalam membantu dan mengambil suatu keputusan dalam melaksanakan tugasnya. Sampel data terdiri dari objek dalam makna yang lebih luas yaitu internal dan eksternal, tersusun dan tidak terstruktur, grafik , suara dan lainnya.

KESIMPULAN

Penerapan risk management terhadap system informasi manajemen merupakan system yang harus di miliki oleh setiap perusahaan dan dikembangkan, sehingga kemunculan kemunculan risiko yang ada akan semakin sedikit. Risk Management Framework Secara umum telah disetujui sebagai kerangka kerja manajemen risiko dalam memberikan informasi kepada sistem informasi manajemen. Risk treatmen memiliki tujuan agar dapat menentukan tindakan yang dilakukan dalam menangani risiko yang telah terdeteksi, supaya mengurangi pengaruh risiko sistem informasi management secara menyeluruh. Proses penilaian risiko pada Risk analysis dapat dilaksanakan menggunakan metode metode yang ada seperti; Bowtie analysis, qualitative analysis atau analisis kualitatif , dan semi quantitative analysis.

DAFTAR PUSTAKA

- Harsanto, Kukuh. & Hidayat, D. 2018. "Sistem Informasi Manajemen Risiko Dengan Menggunakan Framework National Institute Of Standards And Technology Pada Lembaga Pendidikan". Dalam JURNAL IPSIKOM, Vol.6, No.1. Hlm. 1-9.
- Ansori, A. 2017. Penerapan E-Banking Syariah Pada Sistem Informasi Manajemen Perbankan Syariah". Dalam Jurnal BanqueSyar'i, Vol.3, No.1. Hlm. 113-142.
- Yanto, F. & Mardiani, G.T.2018. "Sistem Informasi Manajemen Risiko Proyek Di PT. Pulo Damar Abadi". Universitas Komputer Indonesia. Hlm.1-8.
- Permatasari, D. A ,dkk. 2019. "Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur". Dalam Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol.3, No.6. Hlm. 6001-6008.
- Supradono, Bambang. 2009. "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And

Vulnerability Evaluation)". Dalam jurnal Media Elektrika, Vol.2, No.1. Hlm.4-8.

Mulawarman, A. D., Dkk. 2022. " Aplikasi Sistem Informasi Bank Sampah: Sebuah Studi Kasus". Dalam Jurnal Riset dan Aplikasi : Akuntansi dan Manajemen, Vol.5, No.3. Hlm.273- 284.

Husein, G.M., & Imbar, R.V. 2015. " Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL)". Dalam Jurnal Teknik Informatika dan Sistem Informasi, Vol.1, No.2. Hlm . 75-87.