# Risk Management in Final Semester Exam Information System Using NIST 800-30 Method (Case Study of SMKN 2 Baleendah)

Riyan Farismana*; Dian Pramadhana

***ABSTRACT***

*In the use of information systems and technology, risk is something that must be anticipated. Risks can arise from various things such as information security, fire, hardware damage, etc. that can disrupt the organization's business processes. With the possible emergence of risks in the use of information systems and technology, risk management is needed to facilitate the identification of possible occurrences of these risks. Risk management is the practice of identifying, assessing, controlling and mitigating risks. SMK Negeri 2 Baleendah is a vocational high school that has 5 areas of expertise competence, namely culinary, beauty, fashion, industrial chemistry, and computer network engineering. SMK Negeri 2 Baleendah as an organization engaged in education has implemented online exam information technology. Of course, the application of information technology raises a problem. From these problems, risk management is needed to minimize risk by conducting a risk assessment. NIST 800-30 is a standard document developed by the National Institute of Standards and Technology. NIST 800-30 has two important stages, namely risk assessment and risk mitigation. This research will use the NIST SP 800-30 method as a method that will solve the existing problems. Therefore, a risk assessment was chosen using the NIST SP 800-30 method (Case Study: SMK Negeri 2 Baleendah)*

***Keywords****: information systems and technology; risk management; SMK Negeri 2 Baleendah; NIST 800-30.*

***Correspondence***:
Penulis1
Politeknik Negeri Indramayu, Email; riyanfarismana@polindra.ac.id

## PENDAHULUAN

Dalam penggunaan sistem dan teknologi informasi risiko adalah hal yang harus diantisipasi. Risiko dapat timbul dari berbagai hal seperti keamanan informasi, terjadinya kebakaran, kerusakan hardware,dsb yang dapat mengganggu proses bisnis organisasi (K. J. S. Hoo, 2018). Dengan kemungkinan munculnya risiko pada penggunaan sistem dan teknologi informasi dibutuhkan manajemen risiko untuk memudahkan identifikasi kemungkinan terjadinya risiko tersebut (Karabacak och I, 2017). Manajemen risiko merupakan sebuah praktik mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko (Ekelhart, 2015).

SMK Negeri 2 Baleendah merupakan sekolah menengah kejuruan yang memiliki 5 bidang kompetensi keahlian yaitu tata boga, tata kecantikan, tata busana, kimia

industri, dan teknik komputer jaringan. Sekolah ini menjadi sekolah rujukan yang ditunjuk Kemdikbud yang menjadikan jumlah penerimaan siswa baru selalu bertambah setiap tahunnya. SMK Negeri 2 Baleendah sebagai organisasi yang bergerak dalam bidang pendidikan telah menerapkan teknologi informasi ujian online. Tentu dalam penerapan teknologi informasi tersebut menimbulkan suatu permasalahan. Permasalahan yang pernah terjadi yaitu gangguan pada jaringan client sehingga terputus dengan server,software terjadi error yang dapat mempengaruhi penggunaan aplikasi ujian. Perbaikan dilaksanakan berdasarkan kejadian saat itu terjadi oleh operator IT belum dilakukan pengecekan secara berkala. Dari permasalahan tersebut dibutuhkan manajemen risiko untuk meminimalisir risiko dengan dilakukan penilaian risiko. Manajemen risiko dapat diterapkan sebagai pelindung teknologi informasi dari bahaya keamanan informasi, seperti virus, hacker ataupun pencurian data, menimbulkan ancaman besar terhadap asset dan reputasi perusahaan ataupun organisasi (Fitrianah och. 2016). Ada banyak metode yang dapat digunakan untuk melakukan manajemen risiko keamanan informasi seperti Octave, NIST SP 800-30 dan ISO 27001 (Affandi, 2012). NIST 800-30 adalah dokumen standar yang dikembangkan oleh National Institute of Standards and Technology yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undang-undang Computer Security Act tahun 1987 dan the Information Technology Management Reform Act tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko. Penelitian ini akan menggunakan metode NIST SP 800-30 sebagai metode yang akan menyelesaikan permasalahan yang ada (I. Hermadi, 2014). Maka, dipilih penilaian risiko menggunakan metode NIST SP 800-30 (Studi Kasus: SMK Negeri 2 Baleendah).

## METODE PENELITIAN

Pada penelitain ini, penulis menggunakan NIST 800-30. NIST 800-30 adalah dokumen standar yang dikembangkan oleh National Institute of Standards and Technology yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undang-undang Computer Security Act tahun 1987 dan the Information Technology Management Reform Act tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko. Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu (Syalim, Hori, dan Sakurai, 2009):

**1. System Characterization**

Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.

2. **Threat Identification**

   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.

3. **Vulnerability Identification**

   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.

4. **Control Analysis**

   Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinan-kemungkinan pengembangan dari ancaman.

5. **Likelihood Determination**

   Proses rangking terhadap potensi dari kerawanandapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.

6. **Impact Analysis**

   Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.

7. **Risk Determination**

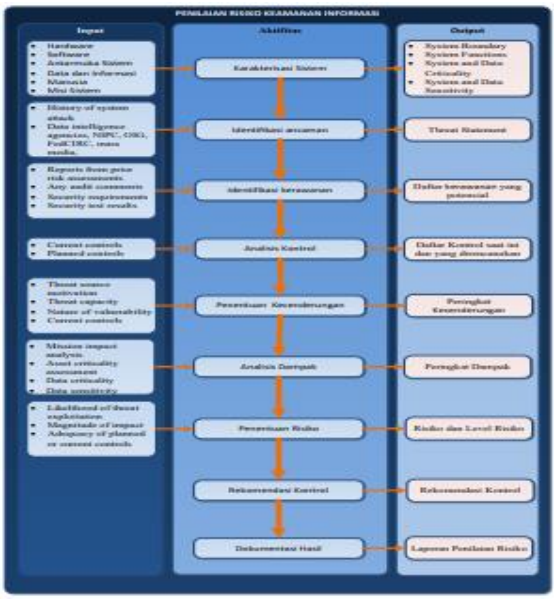
   Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini.

8. **Control Recommendations**

   Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem IT dan data, kepada tingkat risiko yang dapat diterima.

9. **Results Documentation**

   Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko yang dinilai dan kontrol yang direkomendasikan).

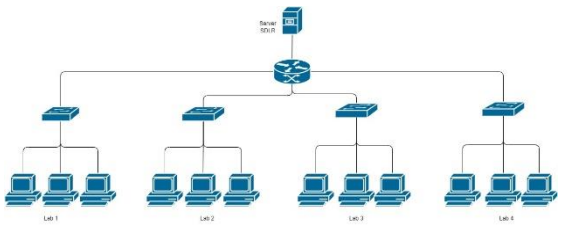



Gambar 1. Penilaian Risiko NIST SP 800-30

## HASIL DAN PEMBAHASAN

## A. System Characterization

Sistem UAS berbasis komputerisasi SDLR SMKN 2 Baleendah hanya bisa dilakukan didalam lab komputer SMK, seluruh host yang terdapat didalam lab komputer terhubung dengan server SDLR yang terletak di lantai 1. Untuk lebih jelasnya dibawah ini merupakan gambar denah lab komputer SMKN 2 Baleendah.



## B. Thread Identification

### 1. History of system attack

History of system attack yang membahayakan sistem dan sering terjadi adalah bahaya banjir, dikarenakan lokasi SMKN 2 baleenddah hanya kurang dari 1 KM DAS Citarum dayeuh kolot.

Tabel 1. Hasil penilaian dari analisis untuk parameter lama, frekuensi dan kedalaman genangan

| Parameter | | Bobot | Skor | Nilai |
|---|---|---|---|---|
| **Lama Genangan** | | 0.5 | | |
| 1-3 hari | | | 0.17 | 0.08 |
| 3-7 hari | | | 0.33 | 0.17 |
| >7 hari | | | 0.5 | 0.25 |
| **Frekuensi Genangan** | | 0.33 | | |
| 1x setahun | | | 0.1 | 0.03 |
| 2x setahun | | | 0.2 | 0.07 |
| 3x setahun | | | 0.3 | 0.1 |
| 4x setahun | | | 0.4 | 0.13 |
| **Kedalaman Genangan** | | 0.17 | | |
| Persawahan | Permukiman | | | |
| <1 m | <15 cm | | 0.1 | 0.02 |
| 1 – 1.5 m | 15 – 25 cm | | 0.2 | 0.03 |
| 1.5 - 2 m | 25 – 50 cm | | 0.3 | 0.05 |
| >2 m | >50 cm | | 0.4 | 0.07 |

### 2. Threat Statement

Dilihat dari history system attack diatas untuk ancaman yang paling sering timbul adalah bahaya banjir yang diakibatkan lokasi SMKN 2 Baleendah berada kurang dari 1 KM dari aliran DAS sungai Citarum, dan yang kedua adalah system crash akibat mati listrik secara tiba tiba.

## C. Vulnerability Identification

Tabel 2. Vulnerability Identification

| **3. Human Disaster** | |
|---|---|
| Penyebab | Kategori |
| - Pencurian | Jarang Terjadi |
| - Hacking | Tidak Terjadi |
| - Tidak adanya SOP | Jarang terjadi |
| - Kesalahan input data | Jarang terjadi |
| **4. Natural Disaster** | |
| - Banjir | Sering terjadi ( Daerah baleendah) |
| - Gempa | Jarang terjadi |
| **5. Technology Disaster** | |
| - Korsleting listrik | Jarang terjadi |
| - Mati Listrik | Jarang terjadi |
| - System crash | Sering terjadi |
| - Virus / Worm | |

## D. Control Analysis

Tabel 3. Control Analysis

| **1. Human Disaster** | | **Kontrol** |
|---|---|---|
| Penyebab | Kategori | |
| - Pencurian | Jarang Terjadi | Pembuatan Tralis |
| - Hacking | Tidak Terjadi | Pembuatan Firewlall |
| - Tidak adanya SOP | Jarang terjadi | Pembuatan SOP |
| - Kesalahan input data | Jarang terjadi | Adanya seleksi data terlebih dahulu |

| | | |
|---|---|---|
| **2. Natural Disaster** | | |
| - Banjir | Sering terjadi ( Daerah baleendah) | Pindahkan lab komputer dan ruang server ke lantai dua |
| - Gempa | Jarang terjadi | Tempatkan lab di bangunan dengan pondasi kuat |
| **3. Technology Disaster** | | |
| - Korsleting listrik | Jarang terjadi | Perbaiki instalasi listrik |
| - Mati Listrik | Jarang terjadi | - |
| - System crash | Sering terjadi | Perbaiki system baik secara HW dan SW |
| - Virus / Worm | | Pasang antivirus |

## E. Likelihood Determination

Tabel 4. Likelihood Determination

| No | Item | Jumlah | Keterangan | Nilai | Risiko | Level |
|---|---|---|---|---|---|---|
| 1 | ADSL Router 4 Port | 1 | | 250000 | Pencurian | Rendah |
| 2 | Mikrotik routerbord RB750 | 1 | Membagi jaringan lantai 1 dan 2 | 600000 | Pencurian | sedang |
| 3 | Switch 24 port | 4 | Melayani pc Lab 1, 2, 3, 4 | 2400000 | Pencurian | sedang |
| 4 | Server SDLR | 1 | Core i5, Ram 8Gb, HDD 1 TB | 15000000 | Pencurian Hacking System crash Banjir Slah input data | Ttinggi |
| 5 | PC Lab | 80 | DualCore, Ram 2 Gb, Hdd 500 Gb | 240000000 | Pencurian System crash Banjir virus | Tinggi |
| 6 | UPS Server | 1 | Untuk server | 8000000 | Pencurian | Rendah |

## F. Impact Analysis

Tabel 5. Impact Analysis

| No | Item | Jumlah | Nilai | Risiko | Level | Dampak |
|---|---|---|---|---|---|---|
| 1 | ADSL Router 4 Port | 1 | 250000 | Pencurian | Rendah | Rendah |
| 2 | Mikrotik routerbord RB750 | 1 | 600000 | Pencurian | sedang | Tinggi |
| 3 | Switch 24 port | 4 | 2400000 | Pencurian | sedang | Tinggi |
| 4 | Server SDLR | 1 | 150000000 | Pencurian Hacking System crash Banjir Slah input data | tinggi | Tinggi |
| 5 | PC Lab | 80 | 240000000 | Pencurian System crash Banjir virus | Tinggi | Sedang |
| 6 | UPS Server | 1 | 8000000 | Pencurian | Rendah | Sedang |

## G. Risk Determination

Tabel 6. Rsik Determination

| No | Item | Jumlah | Nilai | Risiko | Level | Dampak | Skor |
|---|---|---|---|---|---|---|---|
| 1 | ADSL Router 4 Port | 1 | 250000 | Pencurian | Rendah | Rendah | 2 |
| 2 | Mikrotik routerbord RB750 | 1 | 600000 | Pencurian | sedang | Tinggi | 7 |
| 3 | Switch 24 port | 4 | 2400000 | Pencurian | sedang | Tinggi | 6 |
| 4 | Server SDLR | 1 | 15000000 | Pencurian Hacking System crash Banjir Slah input data | Ttinggi | Tinggi | 9 |
| 5 | PC Lab | 80 | 240000000 | Pencurian System crash Banjir virus | Tinggi | Sedang | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | UPS Server | 1 | 8000000 | Pencurian | Rendah | Sedang | 4 |

## H. Control Recommendation

Tabel 7. Control Recommendation

| No | Item | Risiko | Level | Dampak | Skor | Control Recomendation |
|---|---|---|---|---|---|---|
| 1 | ADSL Router 4 Port | Pencurian | Rendah | Rendah | 2 | Pembuatan Tralis |
| 2 | Mikrotik routerbord RB750 | Pencurian | sedang | Tinggi | 7 | Pembuatan Tralis |
| 3 | Switch 24 port | Pencurian | sedang | Tinggi | 6 | Pembuatan Tralis |
| 4 | Server SDLR | Pencurian Hacking System crash Banjir Slah input data | Ttinggi | Tinggi | 9 | Pembuatan Tralis Pembuatan Firewall Perbaiki sistem Pindahkan Server ke lantai dua Koreksi data sebelum di input |
| 5 | PC Lab | Pencurian System crash Banjir virus | Tinggi | Sedang | 5 | Pembuatan Tralis Gunakan deepfreeze |
| 6 | UPS Server | Pencurian | Rendah | Sedang | 4 | Pembuatan Tralis |

## SIMPULAN DAN SARAN

Berdasarkan hasil penilaian risiko dari hasil analisis sebagai berikut :

a. Risiko tinggi yaitu banjir karena lokasi SMKN 2 Baleendah di dekat DAS citarum, penaggulangan hal tersebut adalah memindahkan server dan lab komputer ke lantai dua.
b. Yang kedua adalah pencurian dan instalasi listrik, bisa ditanggulangi dengan pembuatan tralis besi, dan perbaikan instalasi listrik.
c. Dan yang terakhir adalah system crash akibat server rakitan, yang ditanggulang dengan upgrade atau ganti server ke server build up.

## DAFTAR PUSTAKA

K. J. S. Hoo. (2018). “HOW MUCH IS ENOUGH? A RISK MANAGEMENT APPROACH TO COMPUTER SECURITY.

B. Karabacak och I. Sogukpinar. (2017). “ISRAM: information security risk analysis method,” Comput. Secur., vol. 24.

S. F. och T. N. A. Ekelhart. (2015). “AURUM: A Framework for Information Security Risk Management,” Hawaii Int. Conf. Syst. Sci. Hawaii.

D. Fitrianah och Y. G. Sucahyo, ”AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS

XYZ," Jurnal Sistem Informasi MTI-UI, vol. 4, nr 1, pp. 37-46.

M. Utomo, A. H. N. Ali och I. Affandi. (2012). "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," JURNAL TEKNIK ITS, vol. 1, nr 1, pp. A288-A293.

D. Setiawan och M. P. Halilintar. (2015). "Analisis Gangguan Sambaran Petir Terhadap Kerusakan Perangkat IT Pusat Komputer Universitas Lancang Kuning Menggunakan Metode Collection Volume," Pekanbaru.

T. Iskandar och I. Hermadi. (2014). "Audit Proses Perencanaan dan Implementasi Sistem Informasi PT Bank XYZ, Tbk dengan Menggunakan Cobit Framework," Jurnal Aplikasi Manajemen (JAM), vol. 12, nr 14, pp. 572-581.

D. F. och Y. G. Sucahyo. (2015). "AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS XYZ," J. Sist. Inf. MTI-UI, vol. 4, nr.