

KONSEP PARAADIGMA PENERAPAN NIST DAN API DALAM MANAJEMEN RESIKO PADA PERBANKAN

Ova Nurisma Putra

Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK JABAR Bandung
STMIK JABAR

Jl. Soekarno-Hatta No. 777 Tlp. (022) 7335108 Bandung 40293
ova.np@stmikjabar.ac.id

Abstrak

Indonesia adalah negara yang memiliki kekayaan alam nomor satu di dunia, yang sebenarnya memiliki potensi untuk menjadi negara maju, tapi sayangnya banyak hambatan-hambatan yang menghalangi kemajuan tersebut. Salah satu faktornya adalah kondisi keuangan yang sampai saat ini menjadi masalah yang sangat serius.

Perbankan sendiri merupakan perantara keuangan dari dua pihak, yakni pihak yang kelebihan dana dan pihak yang kekurangan dana. Hal tersebut tercermin pada UU RI no. 10 tahun 1998, tanggal 10 November 1998 yang menjelaskan mengenai Perbankan. Menurut UU RI no. 10 tahun 1998 yang dimaksud dengan BANK adalah "badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan dana dari masyarakat dalam bentuk kredit atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak". Seperti pada pengertiannya, yang pada intinya perbankan merupakan badan usaha yang menghimpun dana dari masyarakat dan menyalurkannya kembali ke masyarakat.

Dalam upaya menekan dan mengelola resiko pada perbankan, maka perlu adanya usulan konsep paradigma *framework* manajemen resiko yaitu *framework National Institute of Standards and Technology* (NIST) yang harus diselaraskan dengan 6 pilar Arsitektur Perbankan Indonesia (API). Hal ini bertujuan untuk menjadikan sistem perbankan yang sehat, kuat dan efisien guna menciptakan kestabilan sistem keuangan dalam rangka membantu pertumbuhan ekonomi nasional.

Kata Kunci— NIST, API

Abstract

Indonesia is a country that has the world's number one natural wealth, which actually has the

potential to become a developed country, but unfortunately many of the obstacles that hinder the progress. One of the factors is the financial condition which until now became a very serious problem.

Banking itself is a financial intermediary of two parties, namely the excess funds and the lack of funds. This is reflected in the RI Law no. 10 of 1998, dated November 10, 1998 which describes Banking. According to RI Law no. 10 year 1998 referred to BANK is "a business entity that collects funds from the public in the form of deposits and channel funds from the community in the form of credit or other forms in order to improve the standard of living of many people". As in the sense, in essence banks are business entities that raise funds from the community and channel it back into society.

In an effort to suppress and manage risk in banking, it is necessary to propose the concept of a risk management framework paradigm that is the National Institute of Standards and Technology (NIST) framework that must be aligned with the 6 pillars of the Indonesian Banking Architecture (API). It aims to make the banking system healthy, strong and efficient in order to create financial system stability in order to help the growth of national economy.

Keywords- NIST, API

I. PENDAHULUAN

Perbankan merupakan badan usaha yang menghimpun dana dari masyarakat dan menyalurkannya kembali ke masyarakat. (putracentr.net:2009). Peranan perbankan yang diharapkan dapat memajukan perekonomian di Indonesia. Kerangka kerja yang dirancang untuk mengatasi berbagai resiko terkait penggunaan

teknologi informasi di bidang perbankan, berikut beberapa acuan yang menjadi landasan dalam membuat *framework*. *Framework* tersebut diantaranya adalah Cobit, OCTAVE, ITIL dan NIST. Dalam penelitian ini menggunakan *framework National Institute of Standards and Technology (NIST)* sampai bagaimana implementasi *framework NIST* diterapkan terhadap kasus yang ada pada Bank X.

NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System*. Terdapat tiga proses dalam manajemen resiko yang dikeluarkan oleh NIST yaitu *Risk Identification*, *Risk Mitigation* dan *Risk Evaluation* (Wolingpirayat:2007). Pendekatan dalam pengelolaan manajemen resiko perbankan di Indonesia berdasarkan 6 pilar Arsitektur Perbankan Indonesia (API).

Selama ini pengelolaan manajemen resiko yang diterapkan dalam bidang perbankan masih ada beberapa yang harus dikembangkan dan diperbaiki dalam realisasinya. Hal ini dapat dilakukan dengan melakukan pendekatan dan memahami konsep yang diterapkan dalam manajemen resiko perbankan melalui pendekatan *framework NIST* mengacu pada Arsitektur Perbankan Indonesia (API). Dalam upaya menyelaraskan *framework NIST* dengan API dalam proses pengelolaan manajemen resiko perbankan Indonesia.

II. LANDASAN TEORI

II.1 Resiko

Resiko pada dasarnya merupakan segala sesuatu yang berdampak buruk terhadap organisasi atau perusahaan. Stoneburner menyatakan resiko adalah dampak negatif yang diakibatkan dengan adanya *vulnerability* (kerentanan), berdasarkan dari pertimbangan baik probabilitas maupun dampak kejadian. Terkait dengan dunia keamanan informasi, resiko digambarkan sebagai probabilitas yang menjadi ancaman yang akan mengeksploitasi kelemahan sistem untuk menciptakan kehilangan dari *confidentiality*, *integrity*, dan *avalilability* dari *asset* (Stoneburner, Goguen & Feringa:2002).

II.2 Manajemen Resiko

Manajemen resiko merupakan langkah atau proses yang dilakukan untuk menangani berbagai resiko yang mungkin terjadi. Stoneburner et. al.

berpendapat bahwa manajemen resiko adalah proses mengidentifikasi, menilai dan mengurangi dampak resiko ke level yang dapat diterima organisasi. Dalam konteks TI proses manajemen resiko yang efektif (Firmansyah:2010).

Dalam Firmansyah, beberapa penelitian mengungkapkan, manajemen pada resiko sangatlah bermanfaat karena akan sangat membantu dalam menghindari kerugian akibat terjadi berbagai resiko yang menimpa. Galorath mengungkapkan bahwa organisasi kita akan sukses menjadi lebih baik jika mampu mengantisipasi berbagai potensi kerugian serta mengelola perubahan yang terjadi (Galorath:2006).

Manajemen terhadap resiko dilakukan melalui tahapan-tahapan tertentu. Secara khusus biasanya adalah *Risk Manajemen Framework* atau lebih dikenal dengan *Framework* manajemen resiko. Lebih khusus dalam kaitannya dengan TI adalah *Framework Manajemen Resiko TI*. Merupakan kerangka kerja yang dirancang untuk mengatasi berbagai resiko terkait penggunaan teknologi informasi, berikut beberapa acuan yang akan menjadi landasan dalam membuat *framework*. *Framework* tersebut diantaranya adalah Cobit, OCTAVE, ITIL dan NIST.

II.3 Profil Resiko

Profil resiko adalah dokumen yang dihasilkan dari hasil penilaian atau *Assesment framework* manajemen resiko berupa identifikasi resiko yang mungkin terjadi terhadap pengelolaan organisasi dalam menggunakan TI. Hasil akhirnya berupa jenis resiko yang mungkin terjadi, sumber resiko, kerentanan, kecenderungan dan rating resiko.

II.4 Basel II

Basel II merupakan kerangka permodalan yang diterapkan melalui kombinasi optimal dari 3 aktivitas utama yaitu pelaksanaan pengawasan yang efektif, disiplin pasar yang konsisten serta operasional bank berdasarkan prinsip kehati-hatian. Implementasi Basel II difokuskan pada kesesuaian antara kecukupan modal bank dikaitkan dengan elemen-elemen resiko yang dihadapi dengan memberikan insentif bagi peningkatan kemampuan manajemen resiko. Hal ini diwakili oleh ketiga pilar yaitu *minimum capital requirements*, *supervisory review process* dan *market discipline*. (Bank Indonesia:2006)

II.5 NIST SP 800 – 30

NIST (*National Institute of Standard and Technology*) merupakan organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System*. Terdapat tiga proses dalam manajemen resiko yang dikeluarkan oleh NIST yaitu *Risk Identification*, *Risk Mitigation* dan *Risk Evaluation* (Stoneburner, Goguen & Feringa:2002).

1. Penilaian Resiko

Merupakan langkah pertama dari metodologi manajemen resiko yang dikeluarkan oleh NIST. Organisasi menggunakan penilaian resiko untuk mendefinisikan ancaman potensial dan resiko yang berhubungan dengan penggunaan teknologi informasi. *Output* dari proses ini diharapkan membantu mengidentifikasi bagaimana kontrol untuk melakukan pengurangan dan penghilangan resiko selama proses mitigasi. Proses ini terdiri dari 9 (sembilan) langkah yang harus dipenuhi yaitu (1) *System Characterization*, (2) *Threat Identification*, (3) *Vulnerability Identification*, (4) *Control Analysis*, (5) *Likelihood Determination*, (6) *Impact Analysis*, (7) *Risk Determination*, (8) *Control Recommendations*, (9) *Results Documentation*. Gambar 1.



Gambar 1. Proses NIST (Wolingpirayat:2007)

2. Mitigasi

Merupakan tahap kedua dari proses manajemen resiko yang dikeluarkan NIST melibatkan prioritasasi, evaluasi dan implementasi rekomendasi dari kontrol pengurangan resiko dari tahapan sebelumnya yaitu penilaian resiko. Pengurangan atau biasa lebih dikenal dengan mitigasi merupakan metodologi sistemik yang digunakan manajemen untuk mengurangi dampak resiko. Aktifitasnya

adalah (1) *Prioritize action*, (2) *Evaluate Recommended Control*, (3) *Conduct Cost Benefit Analysis*, (4) *Select Control*, (5) *Assign Responsibility*, (6) *Develop Safeguard Implementation Plan*, (7) *Implement Selected Control*.

3. Evaluasi

Kegiatan evaluasi resiko adalah kegiatan terhadap keberlangsungan proses mitigasi.

II.6 Pengertian Bank dan Perbankan

Bank berasal dari bahasa Italia yang berarti bantu atau pembantu. Namun seiring berjalannya waktu, pengertian bank meluas menjadi suatu bentuk pranata sosial yang bersifat finansial, yang melakukan kegiatan keuangan dan melaksanakan jasa-jasa keuangan. Secara umum bank adalah suatu badan usaha yang memiliki wewenang dan fungsi untuk menghimpun dana masyarakat umum untuk disalurkan kepada yang memerlukan dana tersebut. Adapun pengertian bank menjadi jelas, berikut beberapa definisi menurut para ahli :

Menurut UU No. 10 Tahun 1998, Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Perbankan adalah segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya.

Bank Umum adalah bank yang melaksanakan kegiatan usaha secara konvensional atau berdasarkan prinsip syariah yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas pembayaran. (Kasmir: 2008:25)

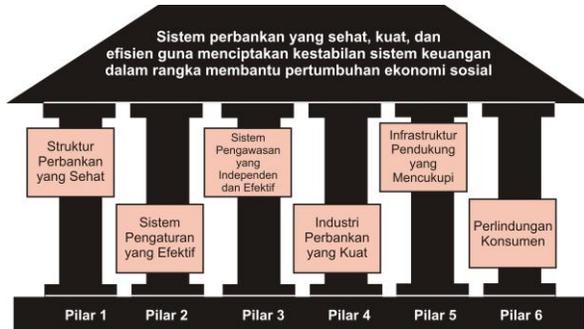
Bank adalah lembaga keuangan berarti bank adalah badan usaha yang kekayaannya terutama dalam bentuk asset keuangan (*financial assets*) serta bermotifkan profit dan juga sosial, jadi bukan hanya mencari keuntungan saja. (Hasibuan: 2005)

II.7 API

Menurut Sari (2010) ada 6 Pilar Arsitektur Perbankan Indonesia (API), meliputi:

1. Pilar 1 : Struktur perbankan yang sehat
2. Pilar 2 : Sistem Pengaturan yang efektif
3. Pilar 3 : Sistem Pengawasan yang Independen dan Efektif
4. Pilar 4 : Industri Perbankan yang kuat
5. Pilar 5 : Infrastruktur Pendukung yang

mencukupi
6. Pilar 6 : Perlindungan Konsumen
Dapat dilihat pada Gambar 2.



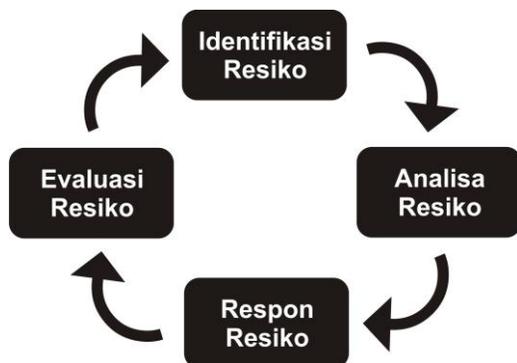
Gambar 2: Enam Pilar Arsitektur Perbankan Indonesia (API) (Sumber: Bank Indonesia)

III. METODE PENELITIAN

Pada penelitian ini langkah-langkah yang dilakukan adalah:

III.1 Mereview Penelitian Terdahulu

Pada umumnya penelitian sebelumnya merekomendasikan framework COBIT, OCTAVE dan NIST untuk analisis resiko TI di perbankan. Seperti yang dilakukan oleh Laluma:2007 membahas tentang membandingkan *framework* manajemen untuk mengelola resiko operasional TI bank yang teridentifikasi. *Framework* yang diusulkan berdasarkan standar **COBIT** (*Control Objectives for Information and related Technology*), **OCTAVE** (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), dan **NIST**, model yang diusulkan ada empat proses meliputi identifikasi resiko, analisa resiko, respon resiko, evaluasi resiko. Gambar 3.



Gambar 3. Model *framework* manajemen resiko operasional

Penelitian berikutnya dilakukan oleh Sari:2010, membahas tentang pengelolaan manajemen resiko perbankan di Indonesia berdasarkan 6 pilar Arsitektur Perbankan Indonesia (API) terdiri dari:

1. Pilar 1 : Struktur perbankan yang sehat
2. Pilar 2 : Sistem Pengaturan yang efektif
3. Pilar 3 : Sistem Pengawasan yang Independen dan Efektif
4. Pilar 4 : Industri Perbankan yang kuat
5. Pilar 5 : Infrastruktur Pendukung yang Mencukupi
6. Pilar 6 : Perlindungan Konsumen

Penelitian yang dilakukan oleh Firmansyah (2010) membahas tentang kerangka kerja yang dirancang untuk mengatasi berbagai resiko terkait penggunaan teknologi informasi di bidang perbankan, berikut beberapa acuan yang akan menjadi landasan dalam membuat *framework*. *Framework* tersebut diantaranya adalah Cobit, OCTAVE, ITIL, NIST, dan lain-lain. Dalam penelitian ini menggunakan *framework* NIST sampai bagaimana implementasi *framework* NIST diterapkan terhadap kasus yang ada pada Bank X.

Perbedaan antara ketiga peneliti sebelumnya terletak pada model *framework* manajemen resiko operasional yang diusulkan ada empat proses meliputi identifikasi resiko, analisa resiko, respon resiko, evaluasi resiko (Laluma:2007). Pengelolaan manajemen resiko perbankan di Indonesia berdasarkan 6 pilar Arsitektur Perbankan Indonesia (API) (Sari:2010) dan implementasi *framework* NIST diterapkan pada Bank. (Firmansyah:2010). Dalam upaya menekan dan mengelola resiko pada perbankan, dapat diidentifikasi faktor-faktor pembanding dalam penerapan manajemen resiko perbankan terletak pada *framework* yang digunakan dalam menentukan resiko perbankan, manajemen resiko operasional yang digunakan dan pengelolaan manajemen resiko perbankan untuk menjadikan sistem perbankan yang lebih baik. Hasil dari review penelitian sebelumnya pada Tabel 1.

Sejauh ini, belum ada yang secara eksplisit mengaitkan antara *framework* analisis resiko TI di perbankan dengan prinsip-prinsip API, sedangkan prinsip API merupakan keharusan pada manajemen perbankan yang dapat diintegrasikan ke *framework*

dan memberikan peluang, solusi, perbaikan dalam penerapan konsep *framework* NIST-API untuk menanggulangi resiko perbankan. Penerapan dan implementasi manajemen resiko perbankan menggunakan *framework* NIST yang diselaraskan dengan 6 Pilar Arsitektur Perbankan Indonesia (API) dengan tahapan-tahapan yang dilakukan lebih sederhana dan mudah dimengerti diselaraskan dengan model Basel II dalam mengelola manajemen resiko operasional perbankan. Adapun tahapan yang dilakukan dalam *framework* NIST adalah: *Risk Identification*, *risk mitigation* dan *risk evaluation* (Wolingpirayat, J.2007).

III.2 Kebutuhan *framework* resiko TI pada perbankan

Perbankan sendiri merupakan perantara keuangan dari dua pihak, yakni pihak yang kelebihan dana dan pihak yang kekurangan dana. Perbankan merupakan badan usaha yang menghimpun dana dari masyarakat dan menyalurkannya kembali ke masyarakat. Dalam upaya menekan dan mengelola resiko pada perbankan, maka harus mematuhi 6 pilar Arsitektur Perbankan Indonesia (API) maka *framework* resiko yang akan diterapkan yaitu *framework National Institute of Standards and Technology* (NIST) harus dapat dipetakan dengan API. Penerapan dan implementasi NIST lebih mudah, selaras dengan Basel II dan dapat dilakukan dengan 3 tahapan yaitu *Risk Identification*, *Risk Mitigation* dan *Risk Evaluation*.

III.3 Teknik Penyelarasan NIST dengan API

Penyelarasan NIST dengan API dilakukan dengan cara, sebagai berikut:

A. Mengidentifikasi langkah-langkah pada NIST

1. Menentukan Penilaian Resiko (*Risk Identification*)

Ada 9 (sembilan) langkah yang harus dipenuhi dalam menentukan penilaian resiko, yaitu :

- a. *System Characterization*
- b. *Threat Identification*
- c. *Vulnerability Identification*
- d. *Control Analysis*
- e. *Likelihood Determination*
- f. *Impact Analysis*
- g. *Risk Determination*
- h. *Control Recommendations*
- i. *Results Documentation*

2. Mitigasi (*risk mitigation*)

Kegiatan yang dilakukan dalam mitigasi, adalah :

- a. *Prioritize action*
- b. *Evaluate Recommended Control*
- c. *Conduct Cost Benefit Analysis*
- d. *Select Control*
- e. *Assign Responsibility*
- f. *Develop Safeguard Implementation Plan*
- g. *Implement Selected Control.*

3. Evaluasi (*risk evaluation*)

B. Pengelompokan NIST pada API

Mengelompokan langkah-langkah pada NIST diselaraskan dengan prinsip pada API, yaitu mengintegrasikan kebutuhan pada tiap pilar yang ada pada API ke *framework* NIST. Tahapan-tahapan ini berdasarkan *framework* NIST, yaitu:

Tahapan *Risk Assesment*, yang dilakukan pada pilar Arsitektur Perbankan Indonesia meliputi:

- Pilar 1 : Struktur Perbankan yang Sehat
- Pilar 2 : Sistem Pengaturan yang Efektif
- Pilar 5 : Infrastruktur Pendukung yang mencukupi

Tahapan *Risk Mitigation*, meliputi:

- Pilar 3 : Sistem Pengawasan yang Independen dan Efektif
- Pilar 4 : Industri Perbankan yang Kuat

Tahapan *Risk Evaluation*, meliputi:

- Pilar 6 : Perlindungan Konsumen

IV. ANALISIS DAN PEMBAHASAN

Berdasarkan metode penelitian pada bab sebelumnya, maka akan dapat di analisis dengan membandingkan kedua konsep tersebut.

IV.1 Analisis

Struktur perbankan Indonesia yang terdiri dari sejumlah bank dengan jumlah kepemilikan aset yang berbeda dapat berdampak pada perbedaan respon yang diberikan terhadap perubahan kebijakan moneter yang diambil oleh bank sentral. Hal tersebut sejalan dengan hasil penelitian yang dilakukan oleh Ruby P. Kishan & Opiela (2000) terhadap perbankan di Amerika Serikat pada tahun 1980 sampai dengan 1995 yang bertujuan untuk membuktikan berjalannya mekanisme transmisi melalui jalur kredit, dengan mengelompokkan bank menurut jumlah aset yang dimiliki dan tingkat *capital leverage ratio*.

Selanjutnya penelitian yang dilakukan oleh Phillip Engler dan Terhi Jokipii (2007) terhadap perbankan Austria pada periode 1997 sampai dengan 2003 yang bertujuan menganalisis bagaimana kelebihan cadangan modal yang dimiliki bank dapat mempengaruhi keputusan pemberian kredit bank serta dampaknya terhadap transmisi kebijakan moneter dari bank sentral terhadap perekonomian di Austria. Kedua penelitian tersebut menunjukkan hasil yang senada yaitu bahwa kelompok bank yang lebih responsif terhadap perubahan kebijakan moneter. Dampak perubahan adalah kelompok bank kecil, hal ini berarti transmisi kebijakan moneter bergerak lebih efektif pada kelompok bank kecil (Sari:2010).

Dari beberapa definisi, kelebihan dan kekurangan dari metode dan *framework* yang digunakan oleh peneliti sebelumnya dapat disimpulkan bahwa manajemen resiko pada perbankan tidak terlepas dari 6 pilar Arsitektur

Perbankan Indonesia (API) yang sudah diterapkan selama ini oleh Bank Indonesia. Untuk menjamin penerapan industri perbankan yang kuat dengan meningkatkan tata kelola bank yang lebih baik, lebih efektif dan efisien dalam menghadapi tantangan global. (BI:2007).

Untuk memperkuat dalam menangani manajemen resiko perbankan perlu dibuat dan dibangun *framework* untuk mengelola resiko operasional TI bank yang teridentifikasi menggunakan standar **COBIT** (*Control Objectives for Information and related Technology*), **OCTAVE** (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), dan **NIST**, model yang diusulkan ada empat proses meliputi identifikasi resiko, analisa resiko, respon resiko, evaluasi resiko, seperti terlihat pada Tabel 2. (Nazir:2005).

Tabel 1. Review Penelitian Terdahulu

No.	Peneliti	Metode	Framework	Keterangan	
				Kelebihan	Kekurangan
1.	Riffa Haviani Laluma	1. Pendekatan kuantitatif, pendekatan berdasarkan nilai-nilai finansial untuk memberikan gambaran tentang kerugian bila sebuah resiko terjadi. 2. Pendekatan kualitatif, pendekatan berdasarkan penilaian institusi, pengalaman terhadap sistem dan resiko-resiko yang dihadapi.	COBIT (<i>Control Objectives for Information and related Technology</i>), OCTAVE (<i>Operationally Critical Threat, Asset, and Vulnerability Evaluation</i>), dan NIST , model yang diusulkan ada empat proses meliputi identifikasi resiko, analisa resiko, respon resiko, evaluasi resiko	Output menghasilkan model untuk identifikasi resiko, analisa resiko, respon resiko, dan evaluasi resiko.	Tidak fokus pada framework mana yang digunakan, hanya memberikan perbandingan antara ketiga framework yang dibahas sesuai dengan standar Basel II
2.	Lisa Kartika Sari	Deskriptif kualitatif, dimana peneliti mengembangkan konsep, menghimpun fakta dan pemahaman tetapi tidak melakukan hipotesis. Pendekatan deskriptif kualitatif digunakan dengan tujuan agar penelitian ini dapat dilakukan secara mendalam sehingga mampu memberikan jawaban atas rumusan masalah yang telah diungkapkan.	1. Implementasi Standar Basel II dengan lebih memfokuskan peningkatan kualitas manajemen resiko di setiap profil resiko dinilai baik bagi pengendalian resiko perbankan (<i>Bank for International Settlement, 2005</i>). 2. 6 Pilar Arsitektur Perbankan Indonesia (API).	Tidak menghilangkan kemungkinan berbagai kendala akan dihadapi oleh perbankan Indonesia baik secara langsung maupun tidak langsung akan berdampak pada keefektifitasan penerapan manajemen resiko tersebut. Dengan pendekatan 6 Pilar Arsitektur Perbankan Indonesia (API).	Tidak membahas dan membandingkan beberapa framework, manajemen resiko untuk mengelola resiko operasional TI.
3.	Hendra	Deskriptif kualitatif	(<i>National Institute of</i>	1. NIST mengeluarkan	Menentukan Level resiko

No.	Peneliti	Metode	Framework	Keterangan	
				Kelebihan	Kekurangan
	Sandhi Firmansyah		Standard and Technology) SP 800 – 30	<ol style="list-style-type: none"> rekomendasi melalui publikasi khusus 800-30 tentang Risk Management Guide for Information Technology System. Terdapat tiga proses dalam manajemen resiko yang dikeluarkan oleh NIST yaitu Risk Identification, risk mitigation dan risk evaluation. Lebih mudah dipahami dibandingkan framework yang lain. 	<p>harus dilakukan terlebih dahulu implementasi secara global terhadap pengelolaan resiko operasional TI.</p>

Tabel 2. Perbandingan framework manajemen resiko dengan model COBIT, NIST dan OCTAVE

Model Basel II	COBIT	NIST	OCTAVE
Identifikasi Resiko	Penentuan Objek, Identifikasi Resiko	Penilaian Resiko: Langkah 1-4	Identifikasi
Analisa Resiko	Penilaian Resiko	Penilaian Resiko: Langkah 5-9	Analisa
Respon Resiko	Respon Resiko	Pengurangan Resiko	Perencanaan dan Implementasi
Evaluasi Resiko	Monitor Resiko	Evaluasi Resiko	Monitor dan Kendali

1. Penilaian resiko (*Risk Identification*)

Organisasi menggunakan penilaian resiko untuk mendefinisikan ancaman potensial dan resiko yang berhubungan dengan penggunaan teknologi informasi. *Output* dari proses ini diharapkan membantu mengidentifikasi bagaimana kontrol untuk melakukan pengurangan dan penghilangan resiko selama proses mitigasi. Proses ini terdiri dari 9 (sembilan) langkah yang harus dipenuhi, yaitu :

a. *System Characterization*

Melihat sudut pandang *hardware, software, interface, data, dan lain-lain*. Sudut pandang inilah yang akan menjadi *input* proses, sehingga akan menghasilkan *output* yaitu batasan sistem, fungsionalitas sistem, data dan tingkat sensitifitas, pengguna dan lain-lain.

b. *Threat Identification*

Mengenali berbagai sumber yang akan menjadi gangguan pada sistem. *Input* dari proses ini biasanya adalah laporan serangan yang pernah terjadi, data dari berbagai pihak baik media, agensi. Sementara *output* dari proses ini adalah *Threat statement*, yaitu merupakan sekumpulan resiko yang mungkin terjadi serta sumber resiko yang dapat menimbulkan kerentanan pada sistem.

c. *Vulnerability Identification*

Pada tahapan ini diidentifikasi berbagai kelemahan atau kekurangan dari sistem yang memungkinkan terjadi ancaman terhadap sistem. *Input* dari tahapan ini laporan dari penilaian resiko terdahulu, bisa jadi serangan yang pernah terjadi, dari hasil pengecekan/pengetesan sistem. Dari pemrosesan dihasilkan *list vulnerability* atau kerentanan yang memungkinkan diserang oleh resiko.

d. *Control Analysis*

Tujuan utama dari tahap ini untuk menganalisis kontrol yang telah diterapkan atau yang akan diterapkan, untuk meminimalisasi kemungkinan terjadinya ancaman. *Input* dari tahapan ini adalah kontrol yang telah diterapkan dalam masing-masing resiko/kerentanan, sementara *outputnya* adalah *list* dari kontrol terhadap resiko yang tengah diterapkan dan rencana kontrol yang akan diterapkan terhadap resiko yang mungkin terjadi.

e. *Likelihood Determination*

Digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi atas kelemahan dari sistem. *Input* dari tahapan ini adalah sumber resiko dan motivasi penyebab sumber resiko, kerentanan dan efektifitas dari kontrol yang diterapkan.

f. *Impact Analysis*

Menilai dampak yang terjadi terhadap serangan atas bagian lemah dari sebuah sistem. *Input* dari sistem ini adalah misi sistem serta tingkat sensitifitas data atau dengan kata lain bagaimana resiko berpengaruh pada misi sistem dan data yang diolah. Kemungkinan yang menjadi pertimbangan adalah masalah integritas data, ketersediaan terhadap layanan dan kehilangan kepercayaan. *Output* dari sistem ini adalah definisi dampak dari resiko (*magnitude of impact definition*).

g. *Risk Determination*

Tujuannya untuk menilai tingkat dari resiko yang timbul pada sistem TI. *Input* dari langkah ini adalah 2 langkah sebelumnya yaitu tingkat kecenderungan dan analisis dampak yang dipetakan menjadi matrik 3 x 3, 4 x 4 atau 5 x 5 tergantung dari kebutuhan sistem. Matriks 3 x 3 melevelkan resiko kepada 3 tingkatan resiko yaitu tinggi, rendah dan sedang (*high, medium, low*). Masing-masing memiliki skor sebagai berikut:

- 1) Probabilitas untuk kecenderungan memiliki level 1.0 untuk tinggi, 0.5 untuk rendah dan 0.1 untuk rendah.
- 2) Nilai untuk tiap dampak adalah 100 untuk tinggi, 50 untuk sedang dan 10 untuk rendah.

h. *Control Recommendations*

Tujuannya untuk mengurangi level resiko pada sistem TI sehingga mencapai level yang bisa diterima. *Inputnya* adalah dari *output* dari tahapan sebelumnya yaitu resiko dan tingkat resiko, dari sini dihasilkan daftar rekomendasi kontrol.

i. *Results Documentation*

Merupakan laporan atau dokumentasi dari seluruh kegiatan yang ada, dimulai tahap karakteristik hingga rekomendasi kontrol.

2. Mitigasi (*risk mitigation*)

Merupakan tahap kedua dari proses manajemen resiko yang dikeluarkan NIST melibatkan prioritasasi, evaluasi dan implementasi rekomendasi dari kontrol pengurangan resiko dari tahapan sebelumnya yaitu penilaian resiko. Pengurangan atau biasa lebih dikenal dengan mitigasi merupakan metodologi sistemik yang digunakan manajemen untuk mengurangi dampak resiko. Aktifitasnya adalah :

a. *Prioritize action*

Berdasarkan hasil dari penilaian resiko dipilih prioritas aksi yang dilakukan. *Input* dari langkah ini adalah level resiko dari tahapan penilaian (*assesment*) yang dilakukan sebelumnya, hasil dari tahapan ini

adalah peringkat prioritas utama yang harus dilakukan terhadap resiko dan kerentanan yang terjadi pada sistem.

b. *Evaluate Recommended Control*

Evaluasi terhadap kontrol yang direkomendasikan dalam proses penilaian resiko, karena bisa jadi rekomendasi yang ditawarkan belum merupakan rekomendasi yang tepat. *Inputnya* adalah kontrol rekomendasi yang ada pada tahapan penilaian resiko, sementara *outputnya* adalah rekomendasi yang paling tepat untuk meminimalisasi resiko yang mengancam sistem.

c. *Conduct Cost Benefit Analysis*

Membantu manajemen dalam pengambilan keputusan dan untuk mengidentifikasi kontrol biaya yang efektif, serta menganalisis keuntungan biaya. *Inputnya* adalah rekomendasi dari tahapan evaluasi kontrol, hal yang dilakukan adalah *cost benefit analysis* terhadap sistem jika dilakukan penerapan rekomendasi kontrol dan *cost benefit analysis* jika kontrol tidak diterapkan

d. *Select Control*

Hasil proses sebelumnya evaluasi terhadap kontrol dan analisis biaya maka dipilih kontrol yang dianggap paling baik dari teknis dan biaya *inputnya* telah jelas adalah *cost benefit analysis*, sementara hasil akhirnya ada kontrol yang terpilih atau akan diterapkan

e. *Assign Responsibility*

Penunjukan personil yang tepat untuk kontrol yang diterapkan, *input* adalah kontrol yang terpilih sementara *output* adalah penugasan atau pemilihan penanggung jawab terhadap kontrol yang dilaksanakan

f. *Develop Safeguard Implementation Plan*

Merencanakan implementasi terhadap kontrol yang diambil, sehingga membantu melancarkan proses pengurangan resiko, dalam tahapan ini rencana implementasi yang aman diterapkan. *Inputnya* adalah resiko dan level resiko, prioritas aksi, kontrol yang dipilih, serta *output* yang menjadi hasil tahap-tahap sebelumnya. Sementara *output* dari tahap ini adalah *safeguard implementation plan guide*.

g. *Implement Selected Control*

Mengimplementasikan kontrol yang dipilih. *Input* nya adalah hasil dari tahap implementasi, sementara *outputnya* adalah pengurangan resiko.

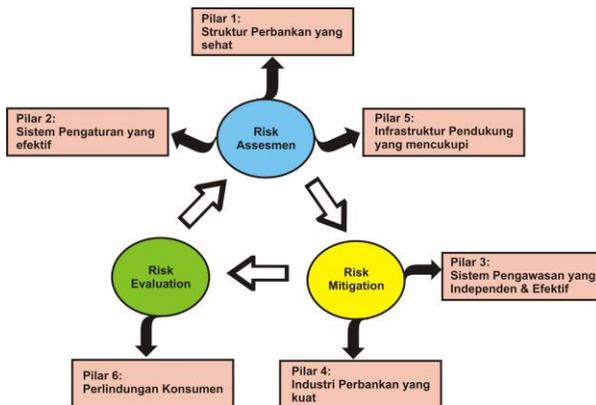
3. Evaluasi (*risk evaluation*)

Kegiatan evaluasi resiko adalah kegiatan terhadap keberlangsungan proses mitigasi, pada

umumnya jaringan yang diterapkan dalam organisasi akan mengalami perubahan atau pengembangan komponen *hardware*, pengembangan *software* dan aplikasi oleh versi yang lebih *up to date* dan lebih baru.

IV.2 Usulan Framework

Dalam upaya menekan dan mengelola resiko pada perbankan. Pada penelitian ini akan diusulkan konsep *framework* manajemen resiko (NIST) harus diselaraskan dengan 6 pilar Arsitektur Perbankan Indonesia (API) pada Gambar 4.



Gambar 4. Skema NIST-API dalam Manajemen Resiko Perbankan

Framework ini diusulkan karena penerapan dalam manajemen resiko perbankan selama ini hanya sebatas satu skema saja belum adanya keterkaitan satu sama lainnya. Oleh karena itu, penelitian ini dilakukan untuk melengkapi dan memperjelas 6 pilar Arsitektur Perbankan Indonesia (API) terintegrasi dalam *framework* NIST. *Framework* ini bertujuan untuk menjadikan sistem perbankan yang sehat, kuat dan efisien guna menciptakan kestabilan sistem keuangan dalam rangka membantu pertumbuhan ekonomi nasional.

Skema NIST-API dalam Manajemen Resiko Perbankan dapat dijelaskan, yaitu:

Tahapan Risk Assesment, yang dilakukan pada pilar Arsitektur Perbankan Indonesia meliputi:

- Pilar 1 : Struktur Perbankan yang Sehat
- Pilar 2 : Sistem Pengaturan yang Efektif
- Pilar 5 : Infrastruktur Pendukung yang mencukupi

Tahap ini dilakukan untuk mengidentifikasi terhadap pilar API yang terdiri dari Struktur

Perbankan yang Sehat, Sistem pengaturan yang Efektif dan Infrastruktur Pendukung yang mencukupi, melalui 9 tahapan yang ada pada aktifitas NIST. Sehingga menghasilkan dokumen yang dapat memberikan informasi tentang kecenderungan dan kelemahan dalam menilai resiko perbankan.

Tahapan Risk Mitigation, meliputi:

- Pilar 3 : Sistem Pengawasan yang Independen dan Efektif
- Pilar 4 : Industri Perbankan yang Kuat

Tahapan ini dilakukan setelah proses *Risk Assesmen*, yang melibatkan prioritasi, evaluasi dan implementasi rekomendasi dari kontrol pengurangan resiko. Dengan melakukan aktifitas berdasarkan sistem pengawasan yang independen dan efektif dan industri perbankan yang kuat. Hal ini membantu dalam menentukan tingkatan pengurangan resiko yang terjadi dengan penunjukan atau pemilihan penanggungjawab terhadap kontrol yang dilaksanakan.

Tahapan Risk Evaluation, meliputi:

- Pilar 6 : Perlindungan Konsumen

Tahapan ini merupakan kegiatan evaluasi resiko terhadap keberlangsungan mitigasi pada umumnya jaringan yang diterapkan pada organisasi yang mengalami perubahan atau pengembangan berupa komponen *hardware*, *software*, aplikasi yang *up to date* dan tidak terlepas dari perlindungan konsumen harus diutamakan selaras dengan Arsitektur Perbankan Indonesia (API) yang diterapkan selama ini.

framework ini, dapat diterapkan melalui tahapan secara berurutan pertama terlebih dahulu menentukan dan mengidentifikasi *Risk Assesment* yang terdiri dari struktur perbankan yang sehat, sistem pengaturan yang efektif dan infrastruktur pendukung yang mencukupi. Kedua adalah *Risk Mitigation* dalam merencanakan sistem pengawasan yang independen dan efektif, diperlukan adanya prioritasi, evaluasi dan implementasi sebagai rekomendasi dalam mengurangi resiko yang terjadi untuk menciptakan peluang industri perbankan yang kuat. Ketiga adalah kegiatan evaluasi resiko terhadap organisasi yang mengalami perubahan dari sumber daya yang ada berupa *hardware*, *software*, aplikasi yang *up to date*. Perubahan ini sangat perlu diberikan perlindungan kepada konsumen yang diselaraskan dengan pilar API sesuai dengan *framework* yang diusulkan.

V. KESIMPULAN DAN SARAN

Berdasarkan kajian melalui proses mencari perbedaan, mengkritik, membandingkan, menggabungkan dan menyimpulkan dari masing-masing *framework* yang digunakan dalam manajemen resiko pada perbankan lebih tepat menggunakan NIST, hal ini tidak terlepas dari 6 pilar Arsitektur Perbankan Indonesia (API) yang sudah diterapkan selama ini oleh Bank Indonesia.

Framework ini dilakukan secara berurutan dari tahapan *Risk Assesment*, *Risk Mitigation* dan *Evaluation*. Setiap tahapan NIST sudah ditentukan pilar API yang terintegrasi sehingga lebih mudah diimplementasikan pada proses manajemen resiko perbankan di suatu Bank. Adapun kendala yang mungkin terjadi pada implementasi *framework* yang diusulkan terletak pada penentuan 6 pilar API yang dijadikan prioritas untuk diintegrasikan ke dalam NIST. Hal ini bisa memberikan peluang, solusi dan perbaikan dalam penerapan konsep *framework* NIST-API untuk menanggulangi resiko perbankan.

REFERENSI

- Bank Indonesia, 2006, Implementasi Basel II di Indonesia, Jakarta: Bank Indonesia.
- Bank Indonesia, 2007, Pedoman Penerapan Manajemen Resiko Teknologi Informasi di Bank Umum, Bank Indonesia, Jakarta.
- Definisi, fungsi dan peran bank umum dalam perekonomian (Tersedia-Online)
<http://putracentner.net/2009/09/23/definisi-fungsi-dan-peranan-bank-umum-dalam-perekonomian/>
- Definisi, fungsi dan peran bank umum dalam perekonomian (Tersedia-Online)
<http://putracentner.net/2009/09/23/definisi-fungsi-dan-peranan-bank-umum-dalam-perekonomian/>
- Firmansyah, H., S., 2010, Implementasi Framework Manajemen Resiko Terhadap Penggunaan Teknologi Informasi Perbankan. Program Studi Teknik Informatika, STMIK Jabar Bandung
- Galorath, D., 2006, Risk Magement Succes Factor. PM World Today. Vol.VIII, Issue 12.
- Hasibuan, Malayu., 2005, Dasar-Dasar Perbankan, Jakarta: Bumi Aksara
- Kasmir, 2008, Bank dan Lembaga Keuangan lainnya, hal 25
- Laluma, R., H., 2007, Penerapan Manajemen Resiko Untuk Bank, STMIK Mardira Indonesia, Bandung, Jurnal Computech & Bisnis, Vol. 1, No. 2, Desember 2007, 84-89, ISSN 1978-9629
- Nazir, M., 2005, Metode Penelitian. Ghalia Indonesia, Bogor
- Pengertian Bank (Tersedia-Online)
<http://banking.blog.gunadarma.ac.id/2010/02/19/pengertian-bank/>
- Sari, L., K., 2010, Penerapan Manajemen Resiko Pada Perbankan di Indonesia. Universitas Negeri Surabaya
- Stoneburner, G., Goguen, A., and Feringa, A., 2002. Risk Management Guide for Information Technology System., Recommendation of National Institute of Standards and Technology Special Publication 800-30.
- Wolingpirayat, J., 2007, *E-payment Strategies of Bank Card Innovation*, Journal of Internet Banking and Commerce.