BAB III
METODOLOGI PENELITIAN

3.1 Objek Penelitian

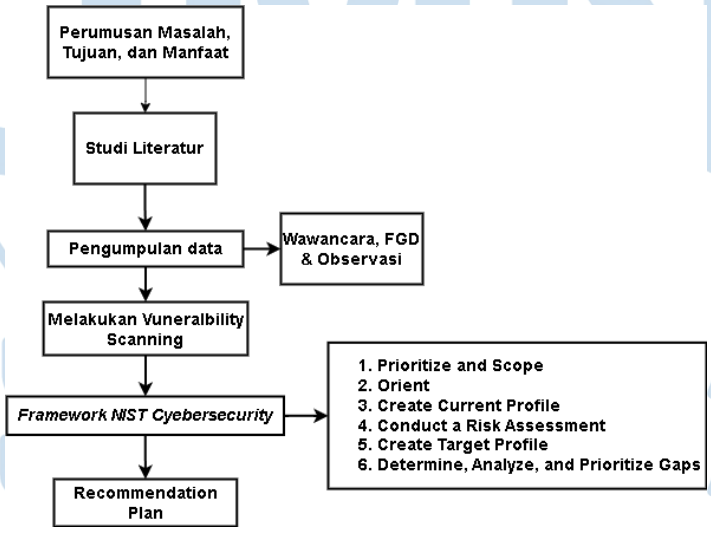
Kerangka pikir penelitian ini dirancang berdasarkan langkah-langkah dari NIST *Cybersecurity Framework* untuk merancang program keamanan sistem layanan PT. XYZ. Gambar dibawah ini adalah gambar tahapan penelitian yang akan dilakukan dalam penyusunan tesis. Tahapan penelitian ini dilakukan secara berurutan. Setiap langkah penelitian yang telah selesai dilakukan, akan mengeluarkan *output. Output* dari langkah penelitian sebelumnya bisa dijadikan sebagai input untuk langkah penelitian selanjutnya.

Gambar 3. 1 Kerangka Pikir

3.2 Langkah- langkah penelitian

Pada penelitian ini, akan dilakukan peningkatan keamanan *cyber* di PT. XYZ. Langka-langkah penelitian yang akan dilakukan dibagi menjadi tujuh langkah, yaitu perumusan masalah, tujuan, dan manfaat, studi literatur, desain proses peningkatan keamanan sesuai dengan *Framework* NIST *Cybersecurity*, pencegahan atau kontrol, dan hasil.

Gambar 3. 2 Kerangka Pikir



a. Perumusan Masalah, Tujuan, dan Manfaat

Berdasarkan diagram alur diatas, hal yang pertama dilakukan adalah perumusan masalah, tujuan dan manfaat. Pada penelitian ini, permasalah yang dihadapi adalah bagaimana menentukan prioritas risiko yang ada?, dan bagaimana meminimalisir risiko keamanan yang terjadi menggunakan *framework* NIST *Cybersecurity* pada Infrastruktur IT PT. XYZ?. Tujuan penelitian ini adalah untuk mengetahui penganan risiko berdasarkan dengan prioritas layanan, menjadikan NIST *Cybersecurity Framework* sebagai standar keamanan *cyber* PT. XYZ. Manfaat yang diharapkan yaitu untuk meningkatkan keamanan, terutama pada sistem operasi dan situs web, mitigasi risiko dapat dilakukan dengan mudah ketika terjadi bencana pada Infrastruktur jaringan karena sudah mempunyai standar yang jelas.

b. Studi Literatur

Langkah berikutnya adalah melakukan studi literatur. Studi literatur dilakukan dengan mencari dan mengumpulkan referensi yang berkaitan dengan penelitian yang dilakukan. Referensi bisa didapatkan melalui jurnal, e-books, dan internet yang membahas tentang *Penetration Testing, Cybersecurity*, dan management risiko.

c. Pengumpulan Data

Pada tahap ini penulis akan mengumpulkan data-data termasuk tentang web *service* seperti sistem dan website yang digunakan PT. XYZ. Pengambilan data akan dilakukan dalam 2 cara, yaitu:

- Observasi

  Penelitian melakukan observasi langsung ke lapangan untuk mendapatkan data.
- FGD (*Forum Group Disscusion*)

  FGD dilakukan bersama dengan 3 orang *staff* dan 1 orang *head division* IT Security untuk mendapatkan data layanan *web* yang tersedia di PT. XYZ. FGD ini akan menggunakan alat ukur yang

di *generate* dari *Framework* NIST *Cybersecurity*. Dalam penelitian ini telah melakukan fgd dan observasi dalam mengumpukan data untuk melakukan klasifikasi keamanan *System* informasi yang ada di PT XYZ. FGD dilakukan kepada seluruh staff divisi *IT Security* yang bekerja di PT. XYZ

d. Melakukan *Vulnerability Scanning*

Setelah melakukan identifikasi layanan, langkah selanjutnya yaitu melakukan *vulnerability scanning* untuk mendapatkan infromasi mengenai 28 vurnerability pada layanan web PT. XYZ. Tujuan melakukan *vulnerability scanning* ini adalah untuk menilai sistem layanan *web* dan situs *web* PT. XYZ. *Vulneralbility Scanning* ini menggunakan tool *WatchTowr*.

Didalam aplikasi web *WatcTowr*, penilaian kerentanan bisa ditemukan pada CVSS (*Common Vulnerability Scoring System*). Penilaian CVSS ini dibagi menjadi 4 kategori beserta rentang penilaiannya. Berikut ini adalah tabel penialaian CVSS:

Table 3. 1 Table Penilaian CVSS

CVSS Severity Level	*CVSS Base Score*
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

e. Prioritize and Scope

Tujuan dari tahap ini adalah untuk melakukan identifikasi fungsi bisnis yang terdapat pada setiap divisi yang ada di bagian IT dan sistem layanan *web* dan *website* yang mendukung proses bisnis divisi tersebut. Dari tahap ini penulis akan mendapatkan sistem layanan *web* dan situs *web* yang sering dipakai dan user mana saja yang mengakses sistem layanan *web* dan situs *web*.

f. Orient

Sesudah mengidentifikasi penggunaan sistem layanan *web* dan situs *web* pada divisi IT, penulis akan melakukan identifikasi segi penggunaan sistem layanan *web* dan situs *web*, level risiko setiap sistem layanan web, dan situs *web*, dan prioritas sistem layanan *web* dan situs *web* tersebut.

Table 3. 2 Tabel Menentukan Prioritas Sistem Layanan

Sistem Layanan/Situs Web	Deskripsi	Penggunaan (H, M, L)	Kriteria Risiko (H, M, L)	Priority Rangking

Dalam penilaian prioritas sistem layanan web dan situs web, dapat dilakukan dengan cara:

- Seberapa sering sistem layanan tersebut digunakan. Contoh L= hanya digunakan pada 1 bagian user. Penulis akan memberikan nilai L=1, M= digunakan 2 bagian user yang berbeda. Penulis memberikan nilai M=2, H= digunakan lebih dari 2 bagian departemen yang berbeda. Penulis akan memberikan nilai H=3
- Dampak risiko yang ditimbulkan. Contoh *High* (H), *Medium* (M), *Low* (L) - Rumus penilaian terhadap *priority rating* sistem layanan adalah Penggunaan * *Risk Rating*
- Semakin tinggi nilai priority rating, sistem layanan web dan situs web tersebut akan dijadikan prioritas dalam melakukan peningkatan keamanannya. Tabel diatas merupakan contoh cara bagaimana menentukan prioritas sistem layanan karena setiap perusahaan atau organisasi memiliki berbagai cara dalam menentukan prioritas sistem layanan.

g. Create Current Profile

Pada tahap ini, penulis membuat profil saat ini menampilka kategori dan subkategori yang termasuk dalam kerangka dasar yang dicapai saat ini. Pada

setiap subkategori akan dilakukan penilaian untuk mengetahui apakah implementasi keamanan *cyber* telah diterapkan dan sesuai dengan keinginan perusahaan.Berikut tabel evaluasi tingkat pencapaian implementasi keamanan *cyber*.

Table 3. 3 Tabel Penilaian Dan Skala Tingkat Pencapaian

Abbreviation	*Description*	*%Achieved*	*Point*
N	*Not Achieved*	*0 to 15% Achievement*	*0*
P	*Partially Achieved*	*>15% to 50% Achievement*	*1*
L	*Lagerlly Achieved*	*>50% - 85% Achievement*	*2*
F	*Fully Achieved*	*>85% - 100% Achievement*	*3*

Sumber: ISO/IEC 15504-2:2003 Section 5.7.2, on pages 10-11, with the permission of ANSI on behalf of ISO. © ISO 2014 - All rights reserved

h. Conduct a Risk Assessment

Pada tahap ini, penulis melakukan penilaian risiko pada sistem layanan, dengan cara mengidentifikasi, menemukan cela keamanan, dan mengklasifikasi masing-masing ancaman yang berpotensi untuk merusak sistem layanan. Proses penilaian risiko akan menggunakan metode penilaian risiko NIST 800-30 [16]. Selanjutnya adalah melakukan analisis kontrol yang sudah ada saat ini, melakukan penentuan kecenderungan terjadinya risiko, melakukan analisis dampak, penentuan risiko, merekomendasikan control berdasarkan tool *WatcTowr*.

Pada tabel di bawah ini menunjukkan parameter nilai kecenderungan terjadinya risiko.

Table 3. 4 Tingkat Risiko

Nilai Kemungkinan	Nilai Dampak		
	Low (10)	*Medium (50)*	*High (100)*
High (1.0)	*Low 10 x 1.0 = 10*	*Medium 50 x 1.0 = 50*	*High 100 x 1.0 = 100*

Nilai Kemungkinan	Nilai Dampak		
	Low (10)	*Medium (50)*	*High (100)*
Medium (0.5)	*Low 10 x 0.5 = 5*	*Medium 50 x 1.0 = 50*	*Medium 100 x 0.5 = 50*
Low (0.1)	*Low 10 x 0.1 = 1*	*Low 50 x 0.1 = 5*	*Low 100 x 0.1 = 10*

Sumber: Stoneburner G, A. Goguen and A. Feringa. (2002). Risk Management Guide for Information Technologt Systems., Reocommendation of the National Institute of : Standart and Technology Special Publication 800-30.

Berdasarkan tabel di atas, kemungkinan terjadinya risiko diberi nilai dengan skala 0.1 sampai dengan 1 dan tingkat besaran dampak dari risiko diberi nilai dengan rentang 10 sampai dengan 100. Setelah tingkat risiko diidentifikasi, rekomendasi manajemen ditentukan untuk mengidentifikasi pengendalian yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi. Tujuan dari tindakan ini adalah untuk meminimalisir tingkat risiko ke tingkat yang dapat diterima. Selain rekomendasi kontrol, proses untuk menanggapi risiko juga ditentukan. Berdasarkan NIST SP-39 perusahaan dapat menanggapi risiko dalam berbagai 4 cara sebagai berikut:[17]

- Penerimaan Risiko Penerimaan risiko adalah penanganan risiko yang tepat ketika risiko yang teridentifikasi berada dalam toleransi risiko perusahaan. Perusahaan dapat menerima risiko yang dianggap rendah, sedang, atau tinggi tergantung pada situasi atau kondisi tertentu.
- Penghindaran Risiko

  Penghindaran risiko dapat menjadi penanganan risiko yang tepat ketika risiko yang teridentifikasi melebihi toleransi risiko perusahaan. Perusahaan dapat melakukan beberapa jenis kegiatan tertentu atau menggunakan jenis teknologi informasi tertentu yang menghasilkan risiko yang tidak dapat diterima.
- Mitigasi risiko

Mitigasi risiko atau pengurangan risiko adalah penanganan risiko yang tepat untuk bagian risiko yang tidak dapat diterima, dihindari, dibagikan, atau ditransfer.

- Berbagi atau Transfer Risiko

  Berbagi risiko atau transfer risiko adalah penanganan risiko yang tepat ketika perusahaan memiliki sarana untuk mengalihkan tanggung jawab risiko ke perusahaan lain. Transfer risiko tidak mengurangi kemungkinan terjadinya peristiwa berbahaya atau konsekuensi dalam hal bahaya terhadap operasi dan aset perusahaan, individu, atau perusahaan lain. Transfer risiko sering terjadi, ketika perusahaan menentukan bahwa mengatasi risiko membutuhkan keahlian atau sumber daya yang lebih baik disediakan oleh perusahaan lain.

i. Create Target Profile

Pada tahap ini, penulis membuat penilaian pada kategori dan subkategori profil target tingkat keamanan *cyber* khususnya pada sistem layanan *web* yang diinginkan perusahaan.

Table 3. 5 Tabel Pembuatan Profil Target

Function	Category	Subcategory	Current *Profile*	Current *Profile*	Target *Profile*
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure the recovery of *Systems* or assets impacted by a *cybersecurity* incident.	RC.RP-1: Rencana pemulihan dijalankan selama atau setelah insiden keamanan *cyber*	F	3	3

	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Rencana pemulihan memasukkan pelajaran yang dipetik	F	3	3
		RC.IM-2: Strategi pemulihan diperbarui	L	2	3

j. Determine, Analyze, and Prioritize Gaps

Setelah mendapatkan data profil saat ini dan profil target, penulis akan membandingkan kedua profil tersebut untuk mendapatkan data gap. Setelah mendapatkan data *gap,* penulis membat *Action Plan* untuk mengatasi *gap* dan mencapai hasil atau target yang telah ditentukan didalam profil target.

k. Recommendation Plan

Penulis membuat tindakan yang direkomendasikan untuk mengatasi *gap*. Setelah membuat rekomendasi, selanjutnya rekomendasi yang telah dibuat akan diserahkan ke Kepala Divisi IT untuk menentukan standar, pedoman, dan praktik yang paling sesuai untuk kebutuhan peningkatan keamanan *cyber* PT. XYZ.