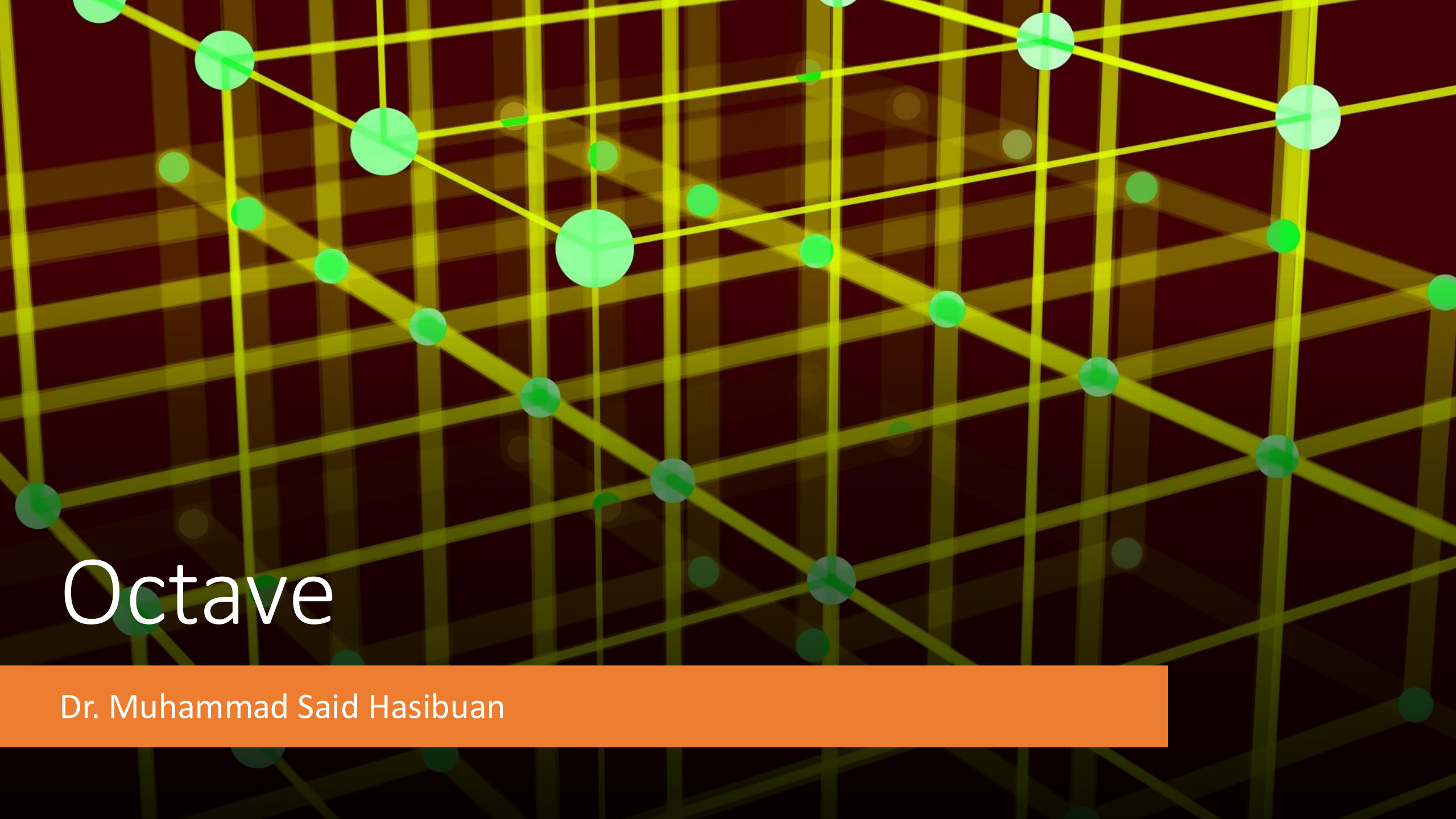


Octave

Dr. Muhammad Said Hasibuan

Octave

- OCTAVE is a methodology for identifying and evaluating information security risks
- OCTAVE Allegro merupakan metode yang menggunakan pendekatan OCTAVE dan dirancang untuk melakukan penilaian risiko terhadap operasional organisasi dengan tujuan menghasilkan hasil yang lebih kuat tanpa perlu mendalami pengetahuan penilaian risiko yang luas

Octave Timeline

Table 1: OCTAVE Timeline

Date	Publication Title
September 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Framework, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S v0.9
March 2005	OCTAVE-S v1.0
June 2007	Introduction of OCTAVE Allegro v1.0

Octave Method Phases

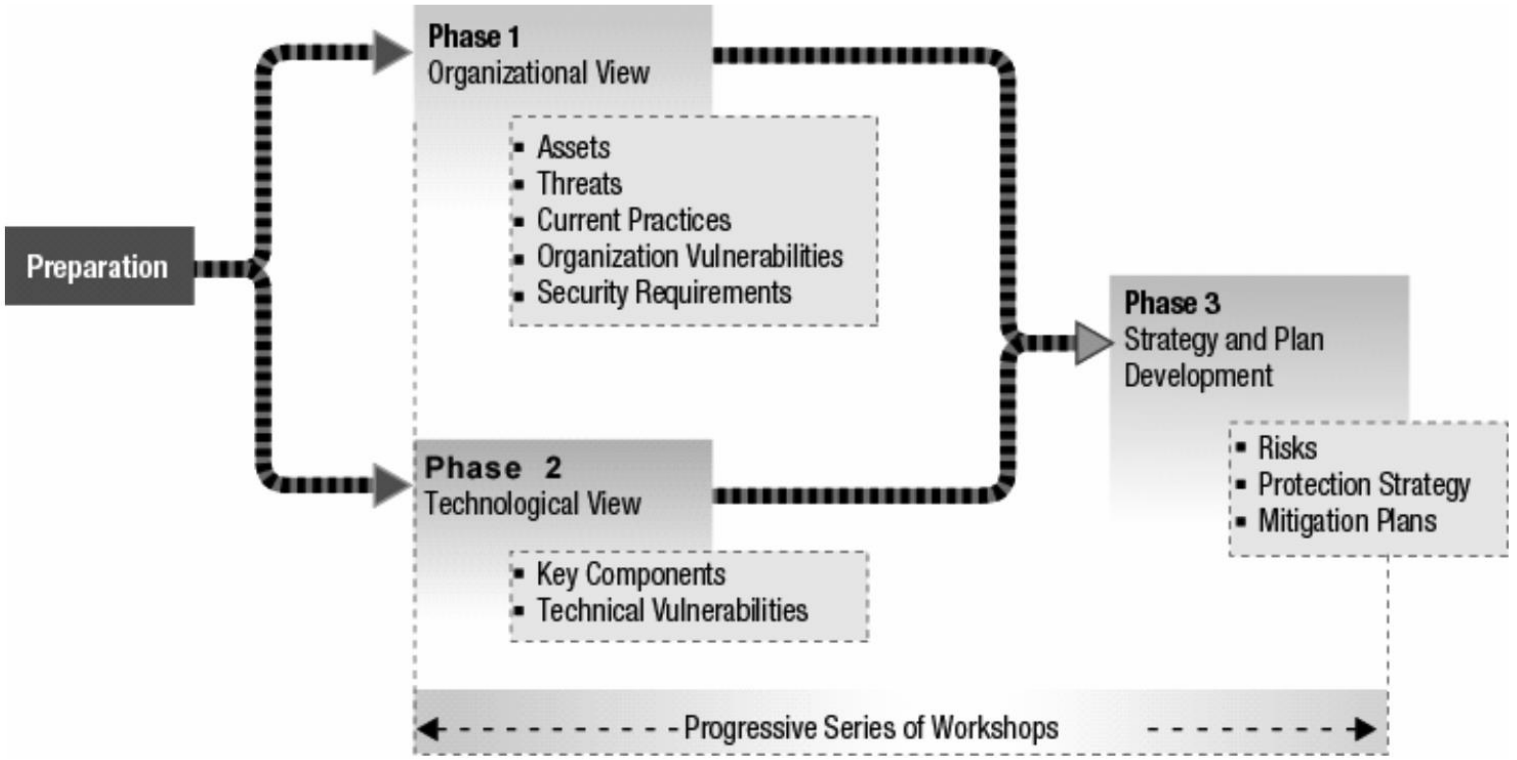
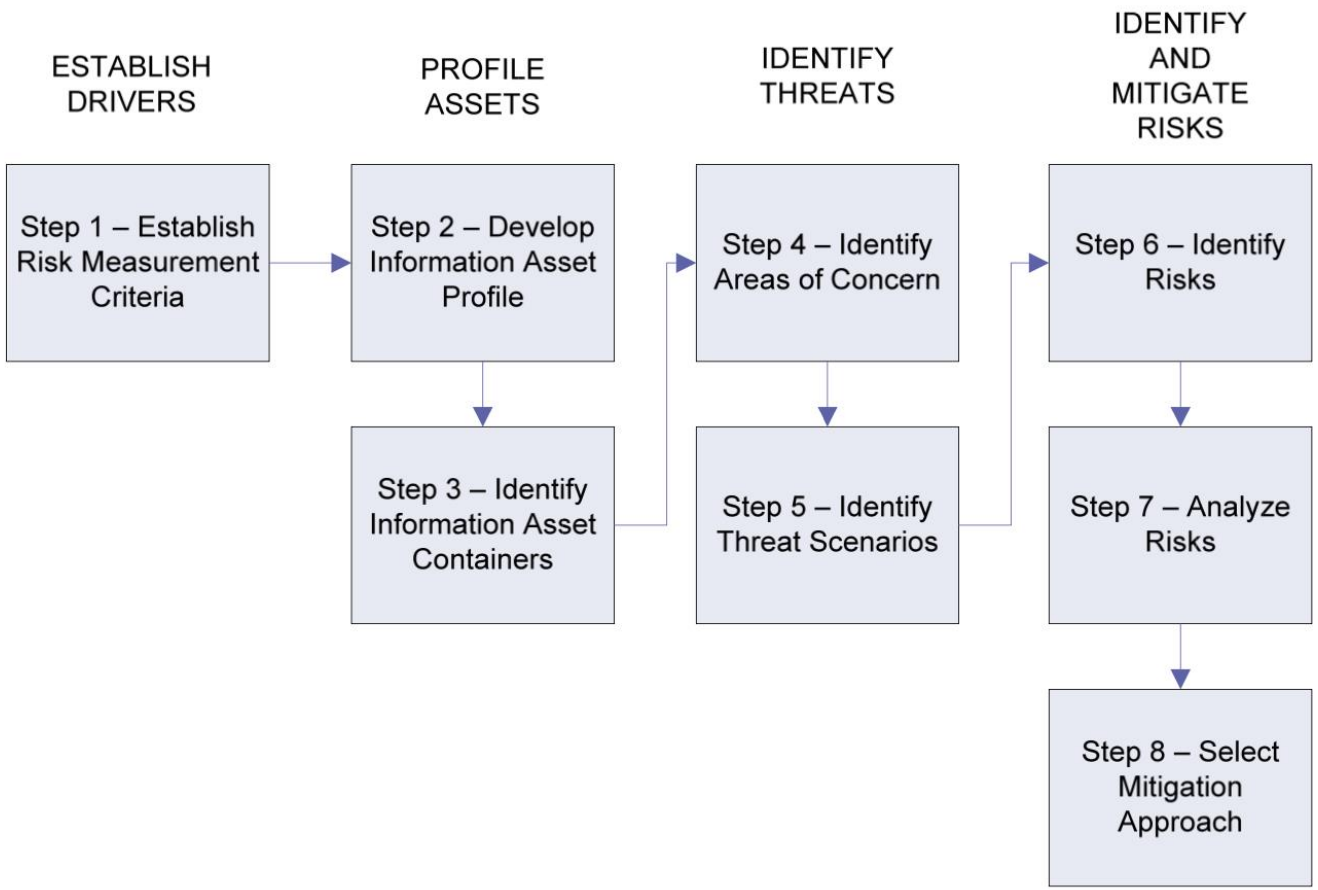


Figure 1: Three OCTAVE Method Phases

Octave Alegro

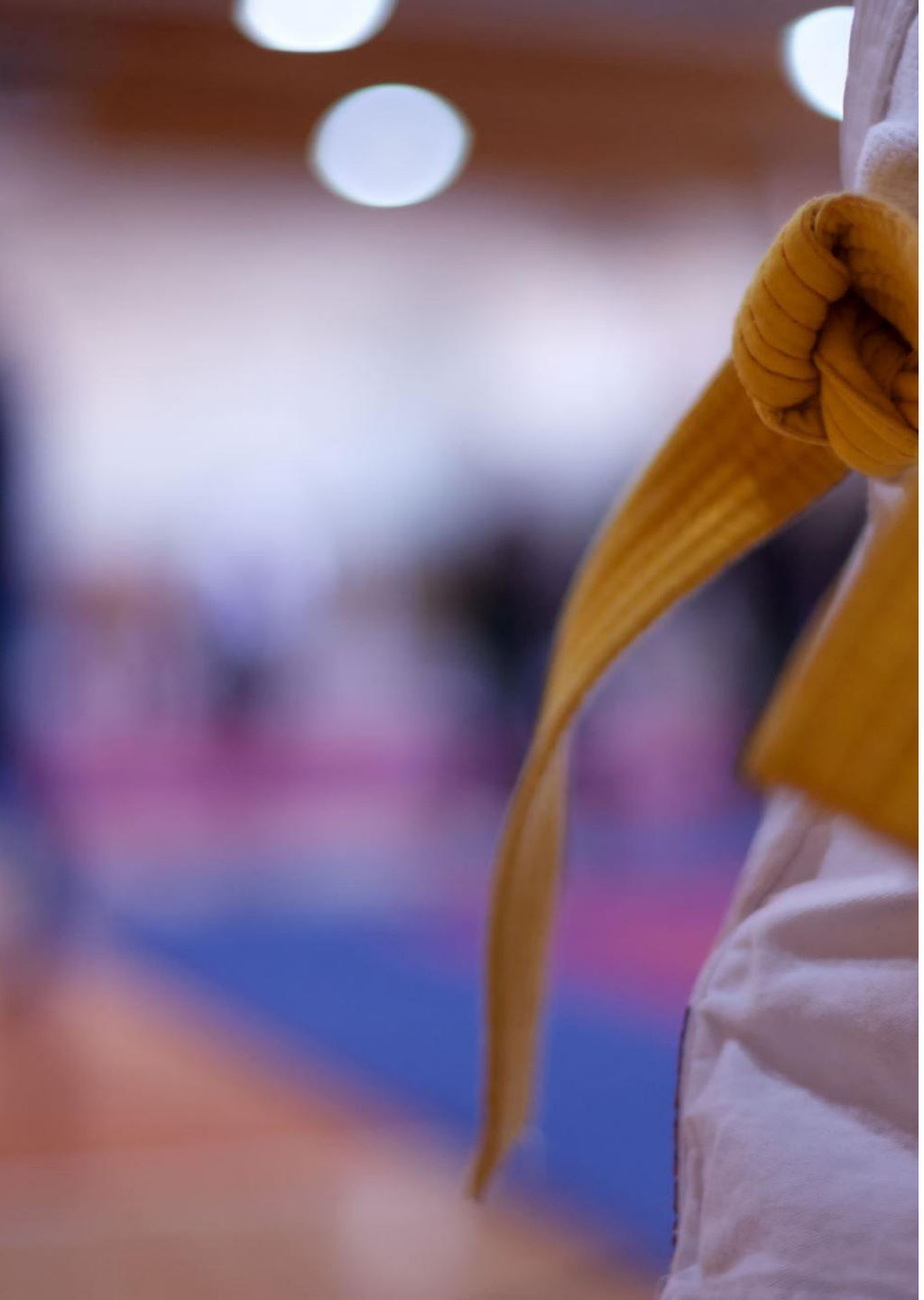


Establish Driver

Menetapkan Risk Measurement Criteria

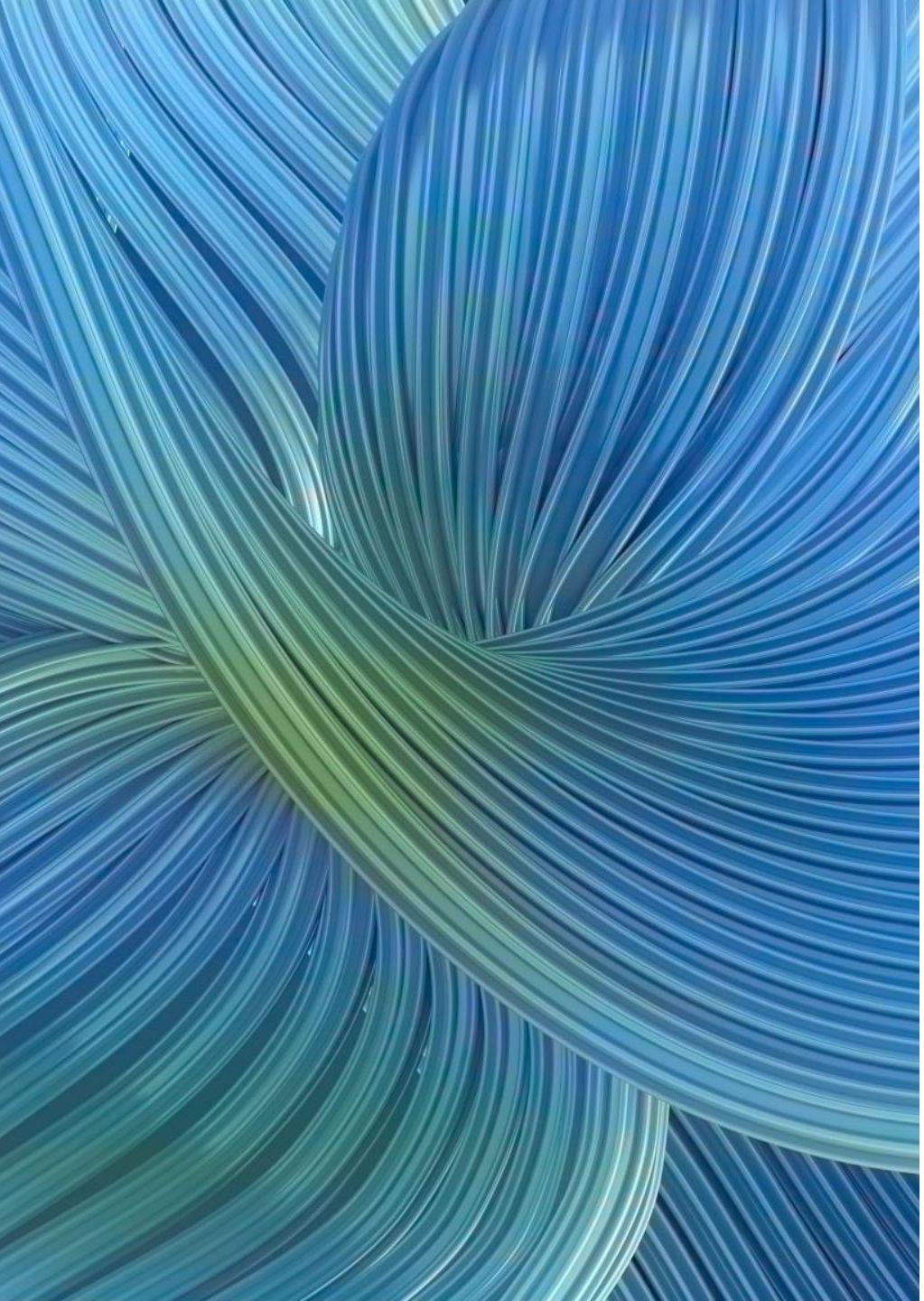
- Pada tahapan ini organisasi atau perusahaan harus menetapkan prioritas dari risk measurement criteria yang telah ditentukan. Mulai dari area yang paling penting sampai yang tidak begitu penting.

Profile Asset



Mengembangkan Profil Aset Informasi

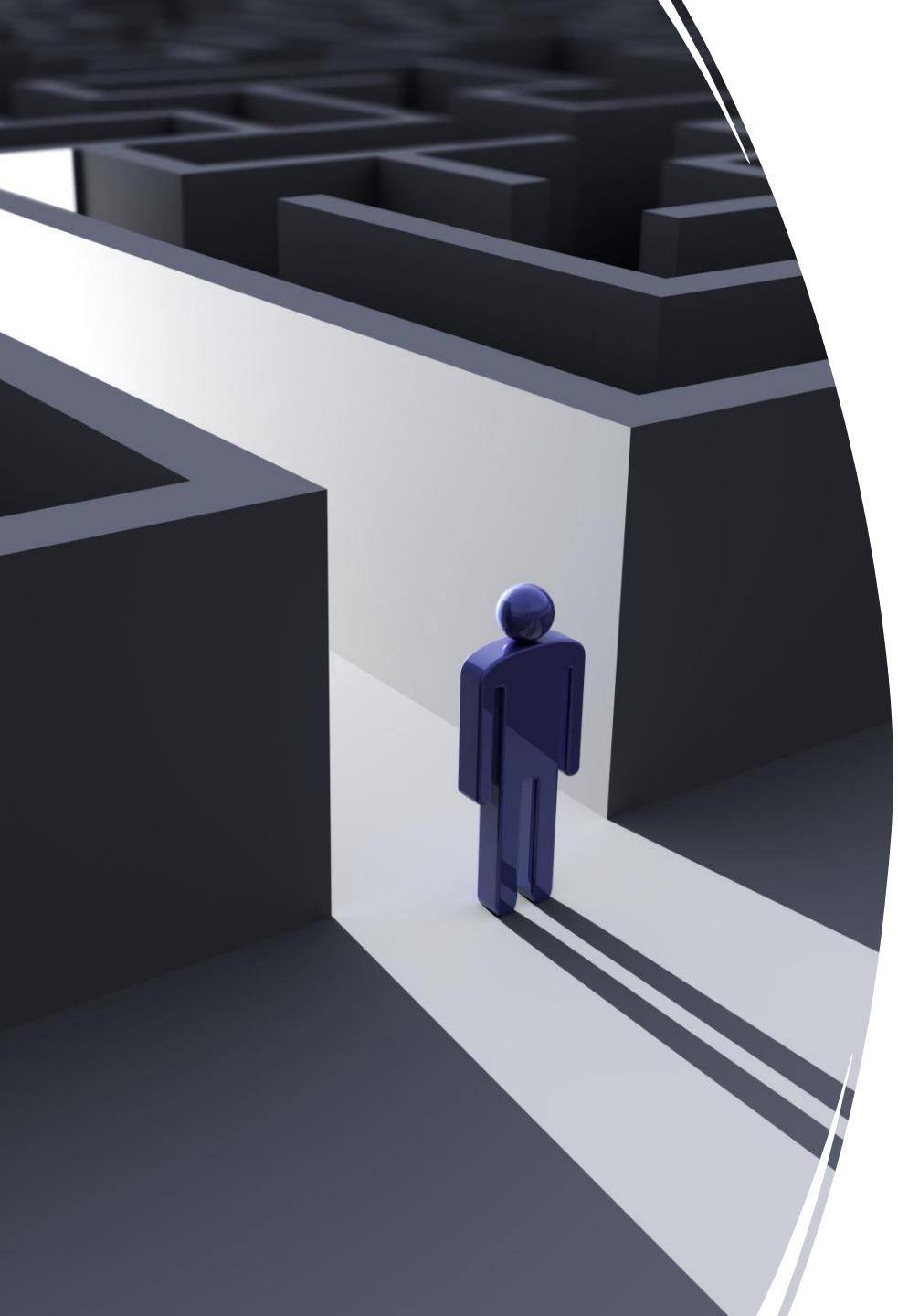
- Pada tahapan ini terdapat beberapa aktivitas yang perlu dilakukan untuk melengkapi profil aset informasi yang akan dibuat yaitu mengidentifikasi sekumpulan aset informasi penting yang mungkin memerlukan penilaian risiko, menentukan aset informasi yang kritikan untuk dilakukan penilaian risiko, dan mengumpulkan informasi yang dibutuhkan terkait aset informasi yang digunakan dalam penilaian risiko antara lain nama aset informasi, alasan pemilihan, deskripsi, pemilik dari aset informasi, security requirement, dan security requirement yang paling penting dari aset informasi tersebut



Mengidentifikasi Containers dari aset informasi

Containers dari aset informasi merupakan tempat dimana aset informasi disimpan, dibawa, dan diproses. Container meliputi aset teknologi (Hardware, Software, Application System, Server, dan Network), folder bekas (tempat dimana aset disimpan dalam bentuk fisik), atau people (yang membawa dan menyimpan aset informasi).

Komponen dari container tersebut dapat berasal dari dalam maupun luar organisasi atau perusahaan. Container yang diidentifikasi terdiri dari tiga tipe yaitu technical, physical, dan people



Identify Threats

Mengidentifikasi Areas of Concern

- Areas of Concern adalah pernyataan yang menjelaskan kondisi atau situasi sebenarnya di dunia nyata yang dapat memengaruhi aset informasi di dalam organisasi atau perusahaan. Pada tahap ini organisasi atau perusahaan perlu mengidentifikasi areas of concern berdasarkan container yang telah ditentukan pada proses sebelumnya

Mengidentifikasi Threat of Scenarios

- Threat scenarios adalah situasi dimana aset informasi dapat dimanfaatkan. Threat scenarios terdiri dari aktor, motif, means (bagaimana aktor melakukannya), dan outcome.
- Pada tahap ini organisasi atau perusahaan dapat membuat skenario–skenario yang dapat mempengaruhi aset informasi untuk masing–masing container yang telah ditetapkan, mengidentifikasi aktor, means, motif, dan outcome, serta menentukan probabilitas terjadinya skenario ancaman

Identify Mitigate Risk

Mengidentifikasi Risiko

- Pada tahap ini, aktivitas yang dilakukan adalah menentukan dampak dari skenario ancaman (threats) terhadap organisasi atau perusahaan.
- Untuk setiap skenario yang telah dibuat, organisasi atau perusahaan harus menentukan dampak atau konsekuensi yang mungkin akan ditimbulkan ketika ancaman (threats) tersebut terjadi.
- Dalam menentukan dampak atau konsekuensi tersebut perlu diperhatikan juga impact area dan hasil yang tidak diinginkan yang telah ditentukan sebelumnya

Menganalisis Risiko

- Pada proses ini, organisasi atau perusahaan mulai mengukur seberapa jauh dampak yang ditimbulkan dari sebuah ancaman (threats) dengan menghitung skor risiko untuk setiap risiko pada setiap aset informasi. Perhitungan skor tersebut digunakan untuk menentukan risiko mana yang perlu dimitgasi terlebih dahulu.
- risk measurement criteria serta definisi high, medium¸dan low yang telah ditentukan dari masing–masing impact area Setelah itu, bandingkan definisi tersebut dengan dampak atau konsekuensi dari skenario ancaman (threats) yang telah dibuat.

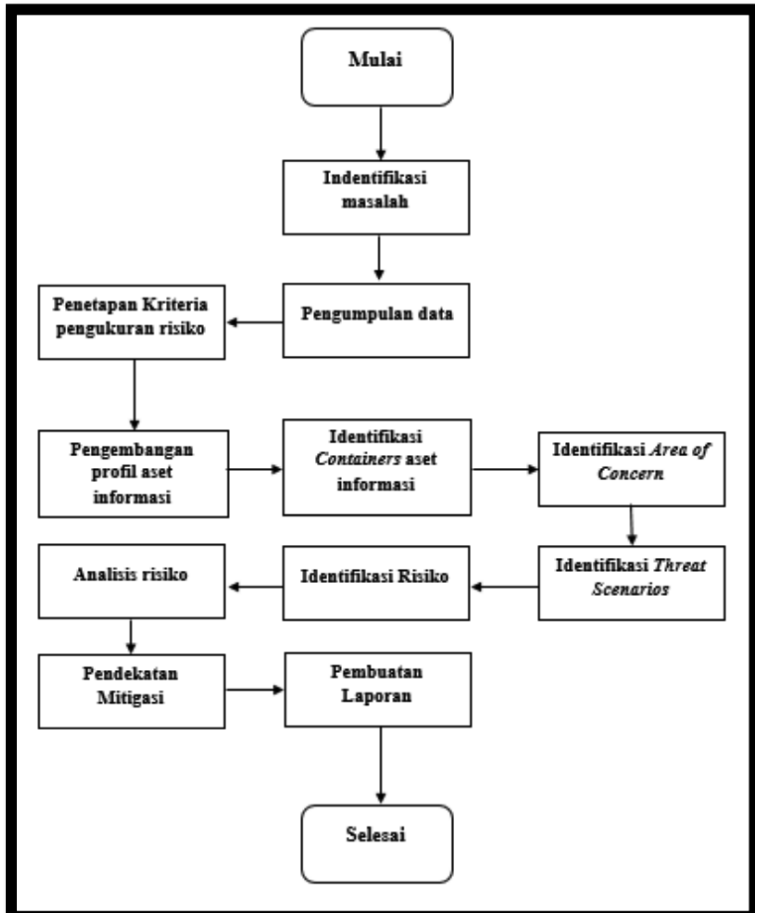
Memilih Pendekatan Mitigasi

- Berdasarkan perhitungan skor pada tahapan sebelumnya, organisasi atau perusahaan dapat menentukan risiko mana yang perlu dimitigasi dan bagaimana caranya.
- Hal tersebut dilakukan dengan membuat prioritas dari risiko, menentukan pendekatan yang akan diambil untuk memitigasi risiko berdasarkan drivers dari organisasi atau perusahaan, dan mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset dan tempat penyimpanannya.

Terdapat tiga aktivitas yang perlu dilakukan pada tahapan ini.

- Pertama, organisasi atau perusahaan perlu mengklarifikasikan setiap risiko yang telah diidentifikasi berdasarkan skor risikonya. Klarifikasi yang dilakukan ini juga perlu memperhitungkan kemungkinan terjadinya risiko tersebut. Dalam pengklarifikasian tersebut digunakan Relative Risk Matrix
- Kedua, tentukan pendekatan mitigasi untuk setiap risiko. Berdasarkan relative risk matrix dari setiap risiko, pilih pendekatan mitigasi yang sesuai untuk organisasi atau perusahaan.
- Ketiga , Dalam mengembangkan strategi tersebut, perlu perhatikan container dimana control akan diterapkan dan residual risk (risiko yang tersisa) setelah control diimplementasikan. Residual risk yang ada harus berada dalam tingkat yang dapat ditoleransi oleh organisasi atau perusahaan.

METODE PENELITIAN



TERIMA KASIH