JAIN DEEMED-TO-BE UNIVERSITY
SCHOOL OF COMPUTER SCIENCE AND IT

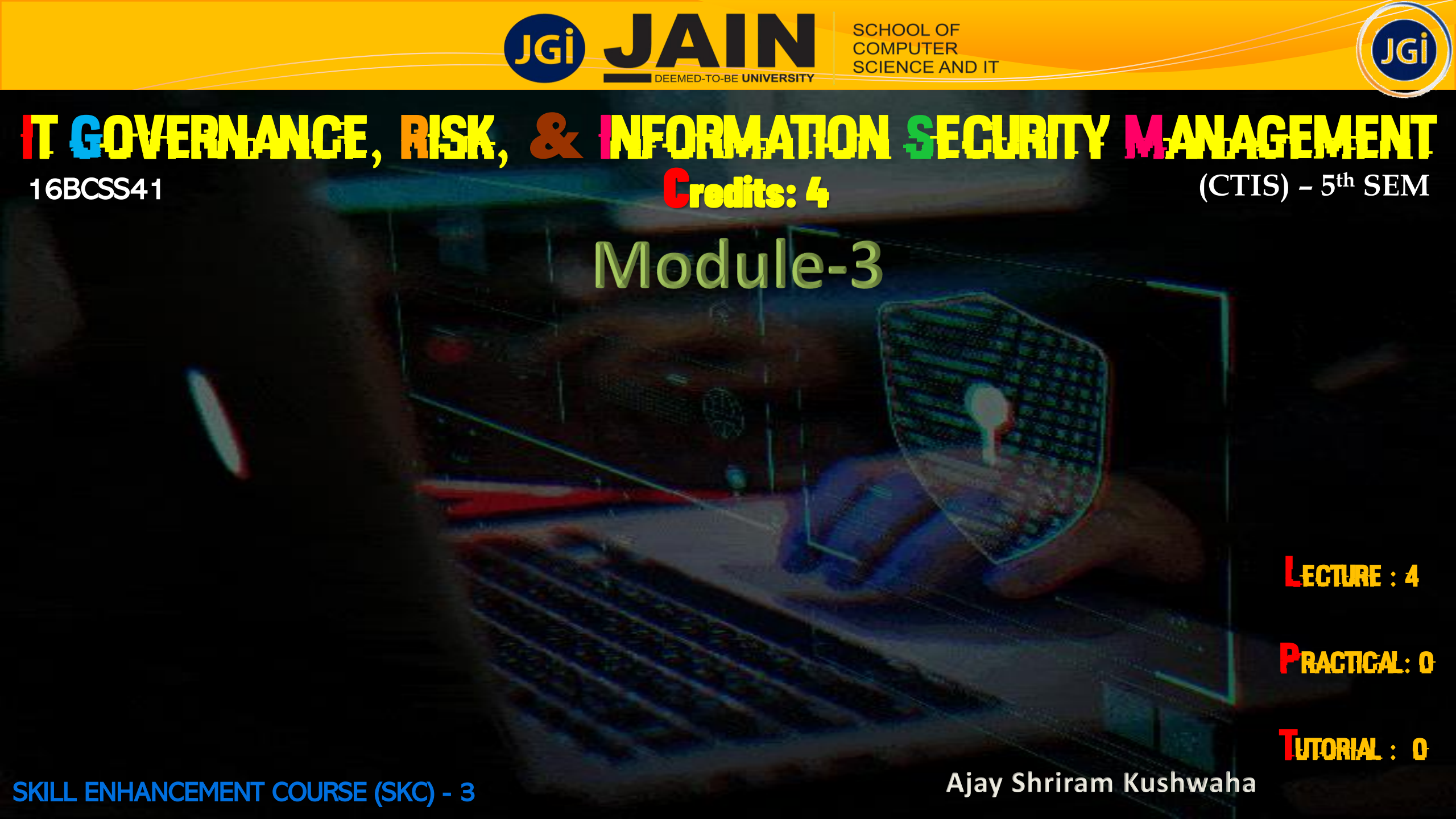
IT GOVERNANCE, RISK, & INFORMATION SECURITY MANAGEMENT

16BCSS41

Credits: 4

(CTIS) – 5th SEM

Module-3



LECTURE : 4

PRACTICAL: 0

TUTORIAL : 0

SKILL ENHANCEMENT COURSE (SKC) - 3

Ajay Shriram Kushwaha

Information Systems Strategy

- Role of Strategic Planning for IT, Role of CISO, Align Security strategy with business objectives, Security Metrics Program

Role of Strategic Planning for IT

What is Strategic Planning?

What is Strategic Planning?

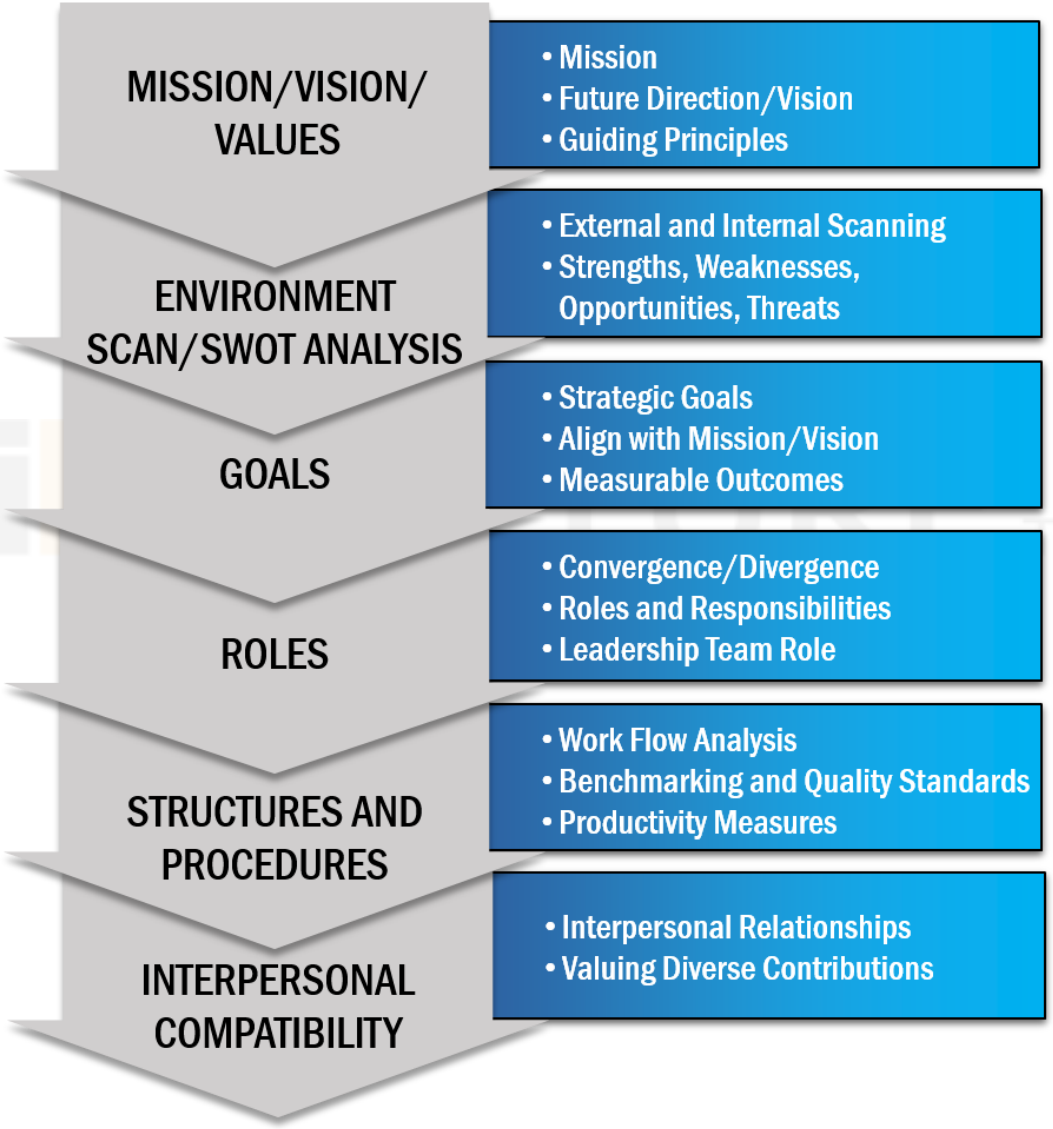
- Strategic planning is an organizational management activity that is used to set priorities, focus energy and resources, strengthen operations, ensure that employees and other stakeholders are working toward common goals.

OR

- A strategic plan is a document used to communicate with the organization the organizations goals, the actions needed to achieve those goals and all of the other critical elements developed during the planning exercise.

Strategic Planning Cycle

Strategic Planning Inter-dependency



Important Role for Strategic Planners

Role	Specifics
Strategic Planning	• Codify - clarify and express - the strategies in terms sufficiently clear to make them fully operational. • Elaborate them into sub-strategies, ad hoc programmes, and action plans. • Convert them - e.g. consider their effects on budgets and performance controls.
Communication & Control	• Communicate strategic intentions - via programmes, schedules, budgets • Control pursuit of them • Gain support of influential outsiders
Finding Strategy	• Help managers find fledgling strategies: • Find patterns • Discover new ways of doing or perceiving things
Analysis	• Analyse specific issues • Provide simple, alternative conceptual interpretations of the world
Catalyst	• Encourage managers to think about the future in creative ways • Get others to question conventional wisdom, and help people out of conceptual ruts.

Steps in Strategic Planning

1) **Analysis or assessment**, where an understanding of the current internal and external environments is developed.
2) **Strategy formulation**, where high level strategy is developed and a basic organization level strategic plan is documented
3) **Strategy execution**, where the high level plan is translated into more operational planning and action items, and
4) **Evaluation or sustainment / management phase**, where ongoing refinement and evaluation of performance, culture, communications, data reporting, and other strategic management issues occurs.

Companies should have the capabilities to:

2) understanding customer value,
3) creating customer value,
4) delivering customer value,
5) capturing customer value, and
6) sustaining customer value.

- **Setting Organizational Direction**
  - The assumption is that organizations ought to plan for the future and set out a path on which to travel.
    - ✓ Where do we want to go?
    - ✓ What do we want to be in the future?

- **Concentration of Effort**
  - An organization needs a means of prioritizing effort and resources.
- **Understanding the Organization**
  - We need to develop an understanding of the culture and history of the organization.
- **Understanding the External Environment**
  - An organization cannot exist without paying attention to the outside world. The phrase "managing from the outside in" sums up the process. The impact of competitors and other external forces needs to be understood;
- **Keeper, Seeker, Disseminator of Information and Values**
  - Information and feedback is at the root of developing learning communities within organizations

Basic Steps in the Management Planning Process

- Identify & Establish Goals
- Prioritize Goals and Tasks
- Identify Resources
- Create Assignments and Timelines
- Establish Evaluation Methods
- Identify Alternative Courses of Action

Relationship of outcomes with Management Directives

CISO	Development & Monitoring
Strategic Alignment	Develop Security strategy and liaise with business unit managers and process owners for ongoing alignment
Risk Management	Ensure risk business impact assessments and develop risk mitigation strategies
Value Delivery	Monitor utilization and effectiveness of security resources and reputation and the delivery of trust
Performance Measurement	Develop and implement monitoring and metrics collection and analysis and reporting approaches
Resource Management	Develop methods for knowledge capture and dissemination. Develop metrics for effectiveness and efficiency
Integration	Liaise with other management process functions. Ensure that gaps and overlaps are identified and addressed.

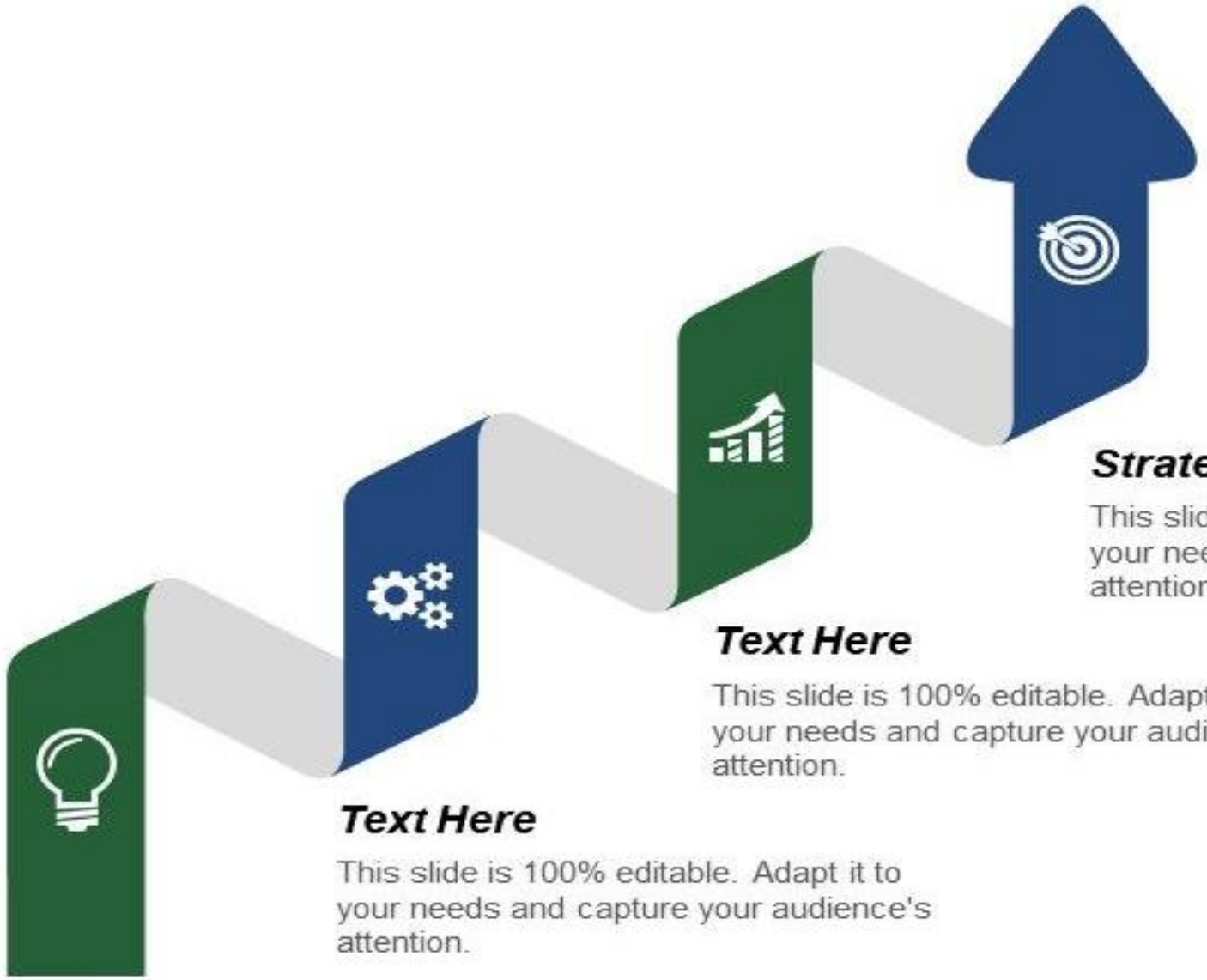
Strategic Direction with Business Objectives

Aligning Security Strategy

- Aligning your cyber security posture with your overall business objectives is essential to protect your business against breaches and intrusions.
- Today, everyone from finance to DevOps to sales and engineering has security top of mind, at least if they know what's good for them.

"Security can be a business driver"

- Align Security with profit
- Know Your Risks
- Support Business Growth at Scale
- Secure doesn't have to Mean Slow



Strategic Direction

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Strategies Development

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Text Here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Text Here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Alignment of Security Strategic with Business Objectives

- By taking a closer look on how these elements are interrelated, it will be easier for you to decide which security controls you should implement for each of them:
- **Business functions will rely on IT assets**
- **IT assets will generate data**
- **Data will provide business functions**
- As an executive, you are responsible for implementing security controls to business functions, IT assets and data.
- You will have to face internal and external risk and base yourself on best practices to protect your business functions, IT assets and data against breaches, intrusions and theft.

Business Function

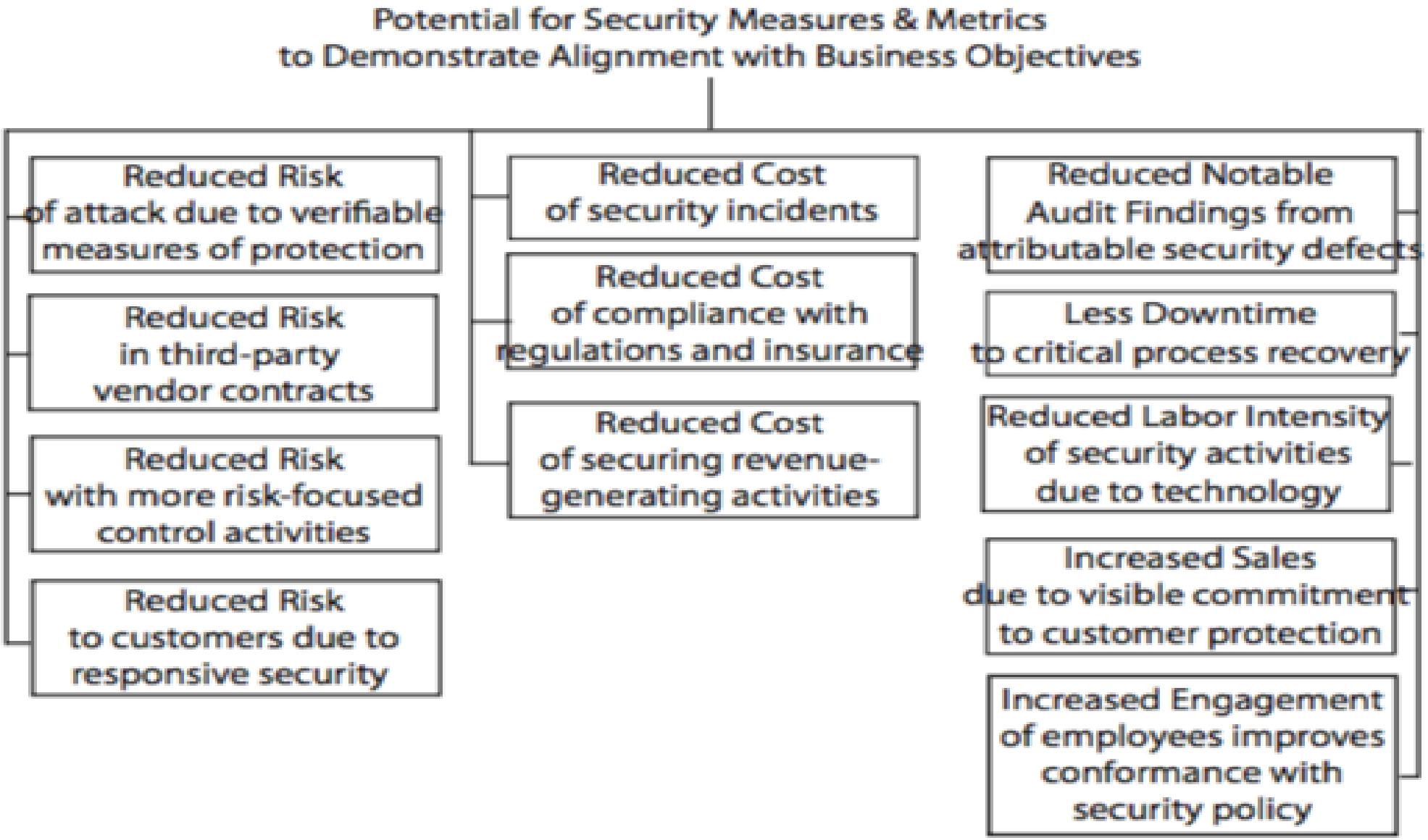
- A business function is a process or operation that is performed routinely to carry out a part of the mission of an organization. Examples includes R&D, Sales, Marketing, HR, Finance, Purchasing, Manufacturing etc.
- We need security controls to protect business functions, which are typically based on governance, management, policies and planning.
- Frameworks: They relate to the norms of the International Standardization Organization (ISO), such as ISO38500 for governance, ISO31000 for business continuity management and ISO22301 for risk, and COBIT 5.
- Related Services: Governance, Management Roles & Responsibilities, Business Continuity Planning, Crisis Management Planning, Risk Management Planning

IT Assets

- IT assets include all elements of hardware and software used in the course of business activities and in the IT environment.
- Examples include operational infrastructure, routers, switches, servers and server components, desktops, mobile devices, backup devices etc.
- Security controls for IT assets are very different to security controls for business functions. You will have to evaluate whether your IT assets are vulnerable to threats and, if so, to which extent:
- Frameworks: Here, you will be able to assess vulnerabilities based on the OWASP Top 10 or CVSS.
- Related Services: Vulnerability Scans, Penetration Testing, Social Engineering

Data

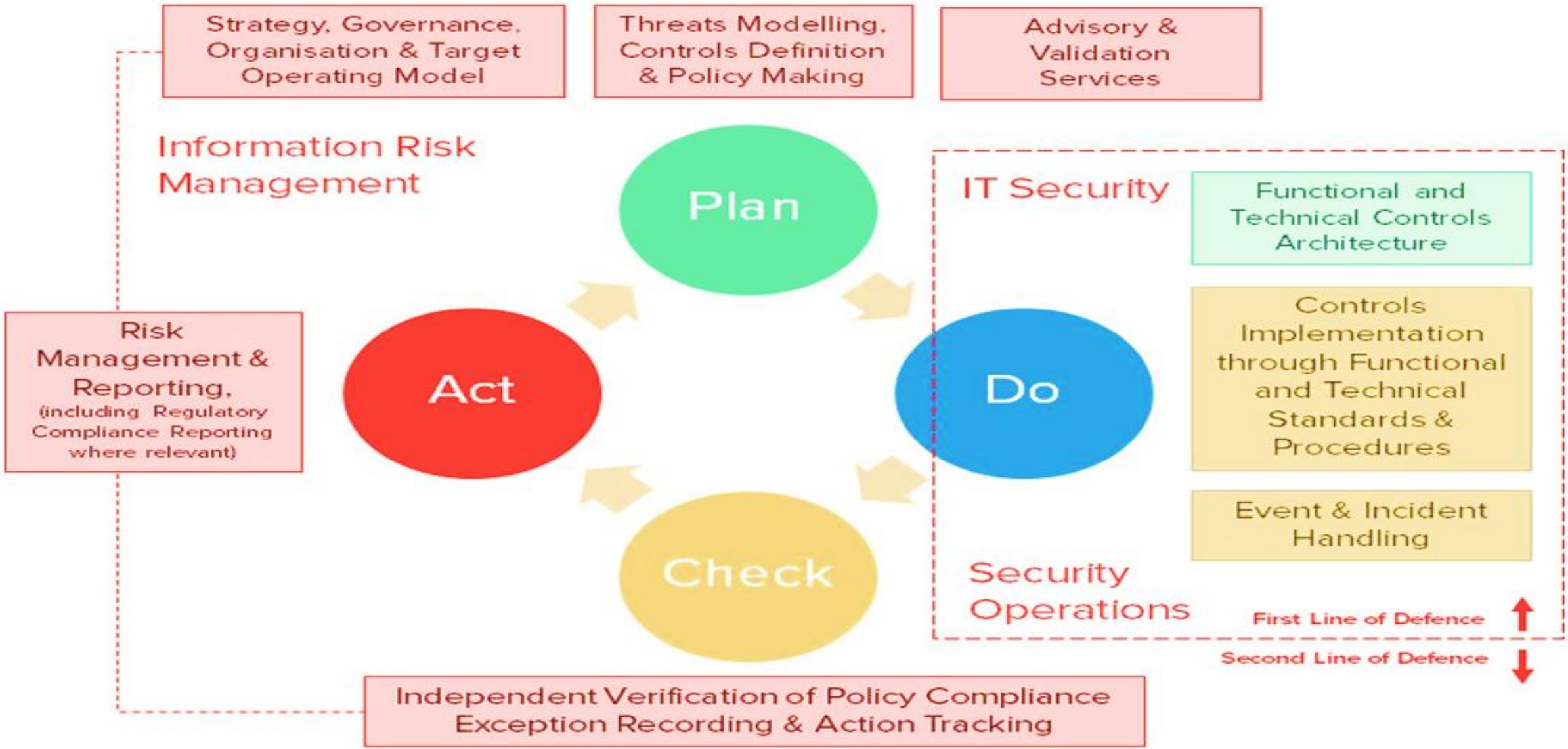
- By definition, data is a collection of facts (numbers, words, measurements, observations, etc.) that has been translated into a form that computers can process.
- In today's digitalized world, businesses use increasingly large amounts of data to carry out their activities and influence their strategic decision making.
- Even with all these security controls in place, you still need to protect your data and deal with data breaches.
- Ideally, organizations should have defined processes in place to monitor their environments continuously and respond to security incidents if needed.


Potential for Security Measures & Metrics to Demonstrate Alignment with Business Objectives
Reduced Risk of attack due to verifiable measures of protection
Reduced Risk in third-party vendor contracts
Reduced Risk with more risk-focused control activities
Reduced Risk to customers due to responsive security
Reduced Cost of security incidents
Reduced Cost of compliance with regulations and insurance
Reduced Cost of securing revenue-generating activities
Reduced Notable Audit Findings from attributable security defects
Less Downtime to critical process recovery
Reduced Labor Intensity of security activities due to technology
Increased Sales due to visible commitment to customer protection
Increased Engagement of employees improves conformance with security policy

Cyber Security is part of Strategic Planning

Role of CISO

Evolving Roles played by CISO



Responsibilities of CISO

- Develop, maintain, and ensure compliance to program
- Designate security officer with primary duties and training
- Develop required policies to support security program and business unit specific needs
- Develop information use and categorization plan
- Assist senior managers with their security responsibilities
- Conduct security awareness

Security Metrics Program

What is Metrics?

A method which facilitates decision-making and improved performance and accountability through collection, analysis and reporting of performance-related data.

Information Security metrics must be:

- based on Information Security performance goals and objectives
- useful for reduction and management of risks
- readily obtainable and replicable
- useful for tracking performance and directing resources
- able to yield quantifiable information

What is Security Metrics?

What Exactly?

- "*Metrics is a term used to denote a measure based on a* reference and involves at least two points, the measure and the reference.
- **Security in its most basic meaning is the protection from or absence of danger.**
- Literally, security metrics should tell us about the state or degree of safety relative to a reference point and what to do to avoid danger."
- When we talk about security metrics we are referring to objective measurements that tell us about our current level of safety and show us how to achieve our goals.

What is our Mission/Goal?

It is critical that we use metrics that are relevant to our organization and to the mission we are measuring.

But first, we have to determine:

- Where we are (Baseline)
- Where we are going (End Goals)
- Who/what relies on us? (Users/Management)
- What do they need/expect? (Reports/Assurance)
- What are we trying to **prove**?
- What are we trying to **solve**?

Why Security Metrics?

Why Security Metrics?

- Gathering available data and turning into useful performance measurement sound like a lot of work, and it's likely that nobody is explicitly asking you to do it.
- So let's make sure we are clear about the benefits you can expect to achieve if you invest time to produce a metrics program.
    - **Security metrics will help you communicate performance**
    - **Security metrics will help drive performance improvement**
    - **Security metrics measure the effectiveness of your IT controls**
    - **Security metrics can guide resource allocation**
    - **Security metrics can demonstrate the state of compliance**
    - **Security metrics can be used to facilitate benchmark comparisons**

How to establish metrics?

Steps to create a metrics program

- In order to create a successful metrics program, an organization should follow these steps:
  - Define the goals and objectives of the metrics program
  - Select the relevant metrics
  - Develop strategies for generating metrics
  - Establish benchmarks and targets
  - Develop a metrics reporting system
  - Develop & implement an action plan
  - Establish a formal program review

Refer the below link to understand more about this:

https://www.happiestminds.com/whitepapers/Buildin-a-Security-Metrics-Program.pdf

What Makes Good Metric?

- "Good metrics facilitate discussion, insight, and analysis; bad metrics prompt furious arguments about methodology."

Good metrics are:

- Necessary to satisfy a specific business requirement
- Consistently measured
- Cheap to produce
- Must yield quantifiable information
- Expressed using at least one unit of measure
- Only repeatable information security processes should be measured
- Contextually specific

Basic Information Security Measures

10

Anti-malware	Firewalls	Asset Management
Intrusion Detection and Prevention	Anti-SPAM	Patch Management
Vulnerability Management	Unified Threat Management	Application Security Scanners
Databases	Website Statistics	Network Access Control
System Integrity Checking	Operating Systems	Data Leakage Protection
Configuration Hardening	Secure Web Gateways	Web Application Firewalls
Mobile Data Protection	Media Sanitation	Storage Encryption

Producing Process oriented Metrics

- Change Management
- Help Desk
- Identity & Access Management
- Incident Response
- Security Awareness Training
- Disaster Recovery & Business Continuity

How can we use Metrics?

- Communicate Performance
- Drive Performance Improvement
- Measure Effectiveness of Security Controls
- Help Diagnose Problems
- Provide Effective Decision-making Support
- Increase Accountability
- Guide Resource Allocation
- Demonstrate the state of compliance
- Facilitate Benchmark Comparisons

Feel Free to ask for Any query

Ajay Shriram Kushwaha