An Implementation Practice of a GRC System Seeking for Value Creation

- COBIT 5 Empowered and Supported the Change -

Yuichi (Rich) Inaba, CISA
（yuichi.inaba@grp.tmnf.jp）

Senior Consultant Specialist
GRC Supporting Dept. and Corporate Planning Dept.
Tokio Marine and Nichido Systems, Co., Ltd.

31 May, 2014

Today’s Contents

1. Introduction – Myself and My Company
2. From Reactive Internal Control to Proactive GRC
3. GRC at Tokio Marine and Nichido Systems
4. COBIT 5 Empowered and Supported the Change

About the Presenter

Yuichi (Rich) Inaba, CISA

Senior Consultant Specialist
GRC Supporting Dept. and Corporate Planning Dept.
Tokio Marine and Nichido Systems, Co., Ltd.

- Have serviced to IT departments at Tokio Marine Group＊

Period	Company	Activities
1992-1998	Tokio Marine Management, Inc（New York）	Overall IT management
1998-2008	Tokio Marine and Nichido Fire Insurance, Co, Ltd	Year 2000 Compliance, System Integration, Project Management, SOX, Risk Management
2008-2011	Tokio Marine Holdings, Co., Ltd.	Implementation and Promotion of Group IT Governance
2011-Present	Tokio Marine and Nichido System, Co. ,Ltd	Implementation, Design and Operation of GRC System

＊）Tokio Marine Group is globally operating Insurance Company Group based in Japan.

Outline of Tokio Marine and Nichido Systems

Established in September, 1983
As a Systems Development Company for Tokio Marine Group

Merged into Tokio Marine and Nichido Systems
In October, 2004, from 3 Systems Companies
Following the Group Merger
Between Tokio Marine and Nichido

1,381 Employees as of April, 2014

Business:
Plan, Propose, Design, Develop, Maintain and Operate the Information Systems of Tokio Marine Group Companies

Webpage URL: http://www.tmn-systems.co.jp/

Corporate Concept of Tokio Marine and Nichido Systems

We deliver the Technology with our whole heart, Globally

To receive the words, Arigatou or Thank you, from the Customers

Management Philosophy

We will be the Value Partner for our Customers that realizes their business utilizing IT and create Values on their business.

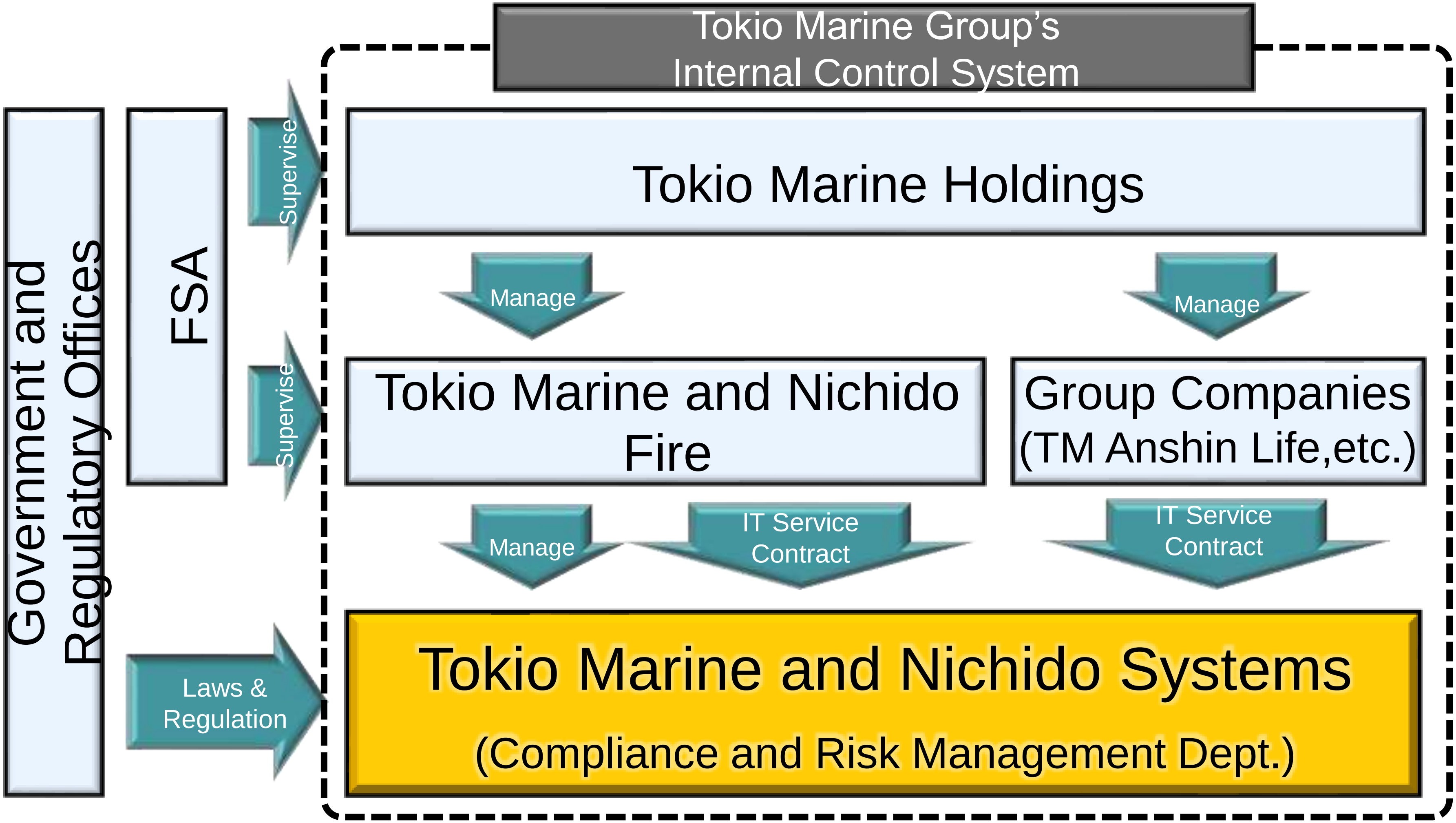
We think the most important resource is human and develop professional human resources that can create Values by using IT.

We focus on communications and create the culture where we can work not only with warm heart and humility but also self confidence and pride.

Today’s Contents

1. Introduction – Myself and My Company
2. From Reactive Internal Control to Proactive GRC
3. GRC at Tokio Marine and Nichido Systems
4. COBIT 5 Empowered and Supported the Change

The Environment Around Us



Government and Regulatory Offices

FSA

Supervise

Supervise

Laws & Regulation

Tokio Marine Group's Internal Control System

Tokio Marine Holdings

Manage

Manage

Tokio Marine and Nichido Fire

Group Companies (TM Anshin Life,etc.)

Manage

IT Service Contract

IT Service Contract

Tokio Marine and Nichido Systems

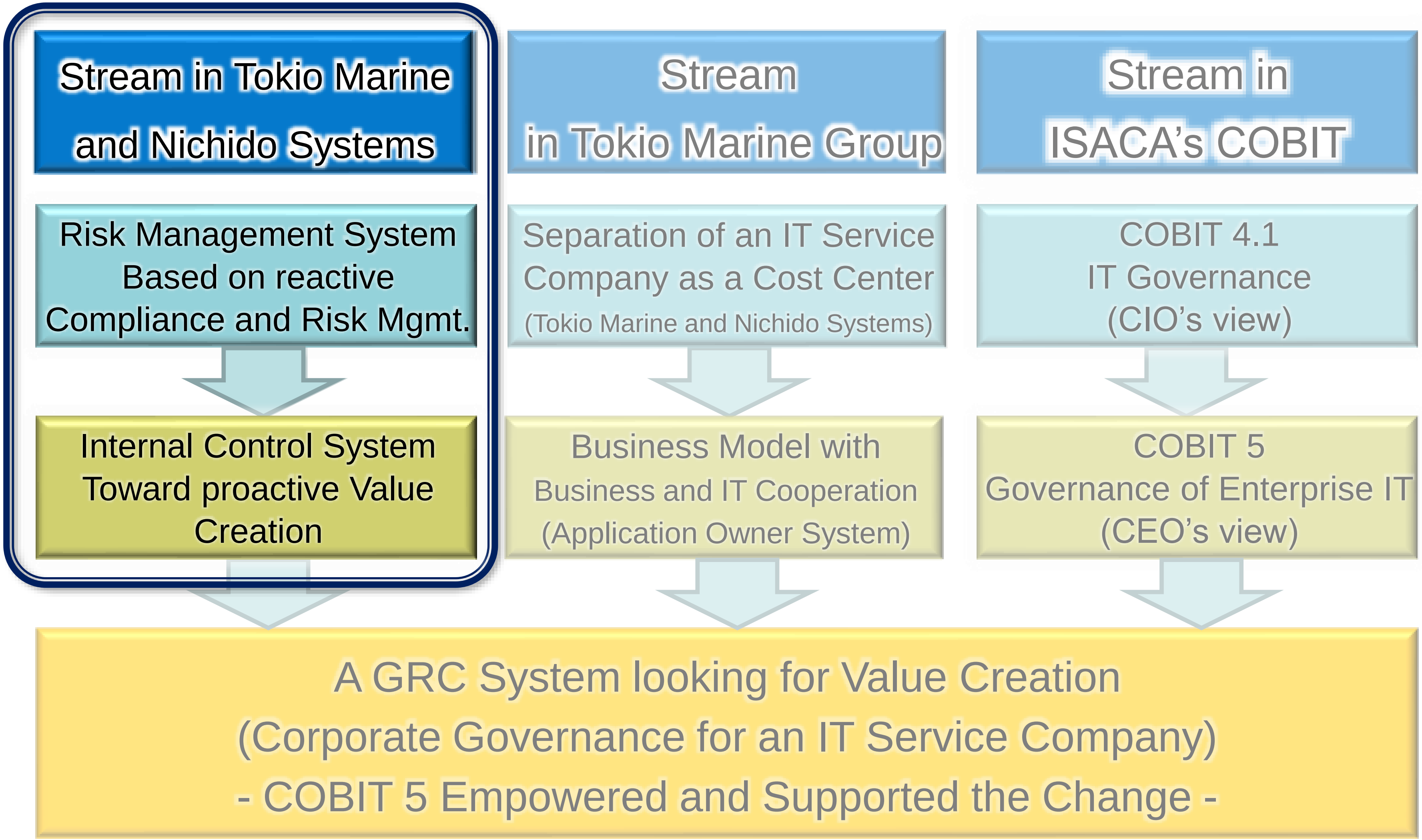
(Compliance and Risk Management Dept.)

Reactive Compliance & Risk Management

Requirement from the External Stakeholders

Stakeholders	Relations	Reactive Actions
Tokio Marine Group Companies	Customers	- Comply with IT Service Contract - Support Customer's Compliance and Risk Management
Tokio Marine and Nichido Fire Insurance	Shareholder (Manager)	- Meet the shareholders expectations (Approvals in advance, Reports)
Tokio Marine Holdings	Holding Company (Group Manager)	- Comply with Tokio Marine Group Governance (Design and Operate Internal Control System)
Government (FSA, etc.)	Regulators	- Comply with Laws and Acts - Comply with FSA's Insurance Inspection Manual

Streams toward the GRC system for Value Creation



Stream in Tokio Marine and Nichido Systems

Risk Management System Based on reactive Compliance and Risk Mgmt.

Internal Control System Toward proactive Value Creation

Stream in Tokio Marine Group

Separation of an IT Service Company as a Cost Center
(Tokio Marine and Nichido Systems)

Business Model with Business and IT Cooperation
(Application Owner System)

Stream in ISACA's COBIT

COBIT 4.1
IT Governance
(CIO's view)

COBIT 5
Governance of Enterprise IT
(CEO's view)

A GRC System looking for Value Creation
(Corporate Governance for an IT Service Company)
- COBIT 5 Empowered and Supported the Change -

Reactive Compliance and Risk Management

Corporation Law

Need to Comply with Tokio Marine Group's Internal Control System

FSA Regulation
(Insurance Inspection Manual)

Need to Support Group Companies' Compliance and Risk Management

Feel that Internal Control, Compliance and Risk Management are too Negative

It is Comfortable to do nothing other than Risk Mitigation and Regulatory Compliance, but …

Wonder if we have a bright future ???

Towards Proactive Internal Controls for Value Creation

Reactive Internal Control – Uneasiness of Company’s future

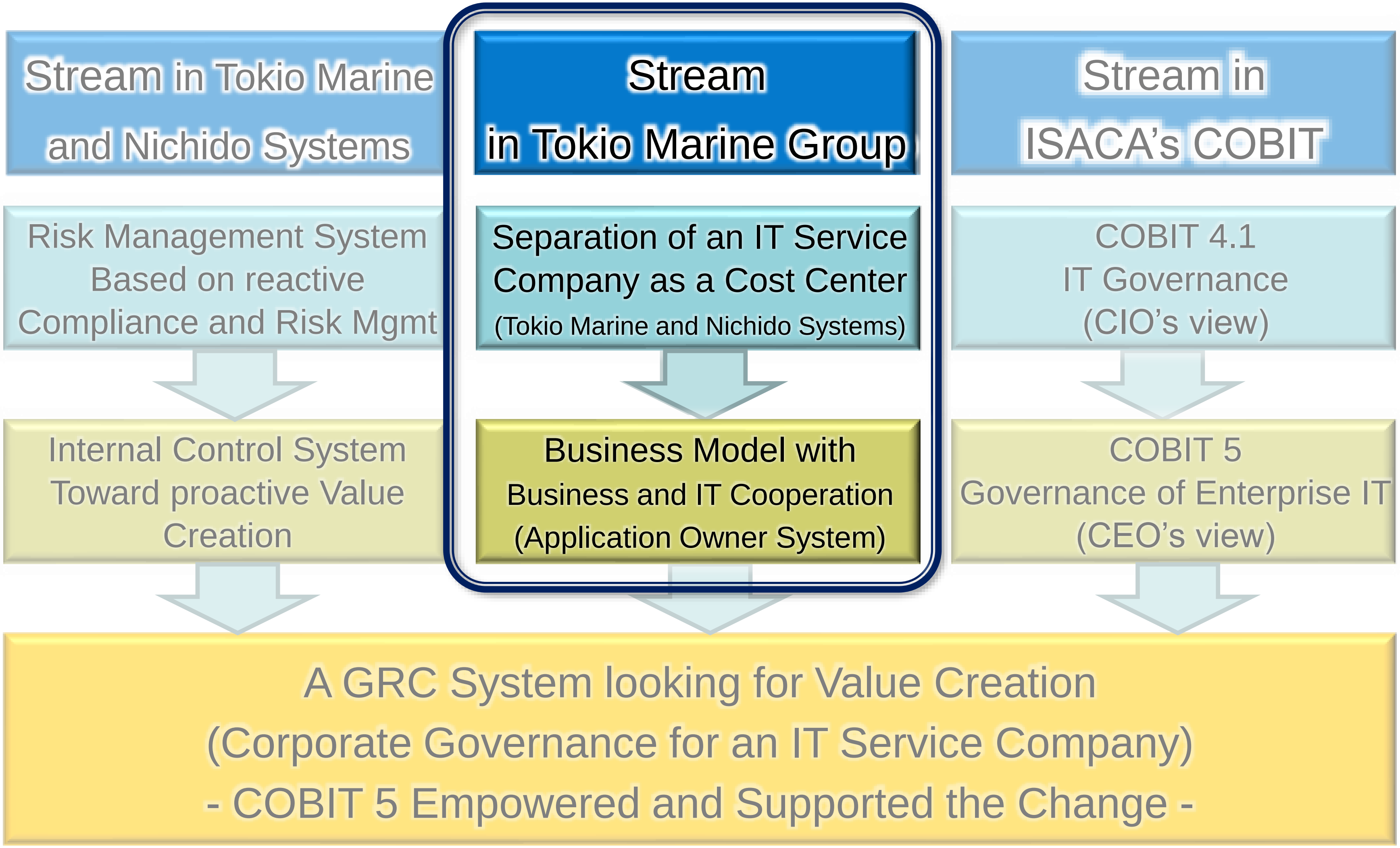
Share the Emotion and Create Customers’ Value Together

Enable to Perform the Business Energetically with Quick Actions

Develop Human Resources and Create Corporate Values

Proactive Internal Controls looking for Value Creation

Streams toward the GRC system for Value Creation



Stream in Tokio Marine and Nichido Systems

Risk Management System Based on reactive Compliance and Risk Mgmt

Internal Control System Toward proactive Value Creation

Stream in Tokio Marine Group

Separation of an IT Service Company as a Cost Center (Tokio Marine and Nichido Systems)

Business Model with Business and IT Cooperation (Application Owner System)

Stream in ISACA's COBIT

COBIT 4.1 IT Governance (CIO's view)

COBIT 5 Governance of Enterprise IT (CEO's view)

A GRC System looking for Value Creation
(Corporate Governance for an IT Service Company)
- COBIT 5 Empowered and Supported the Change -

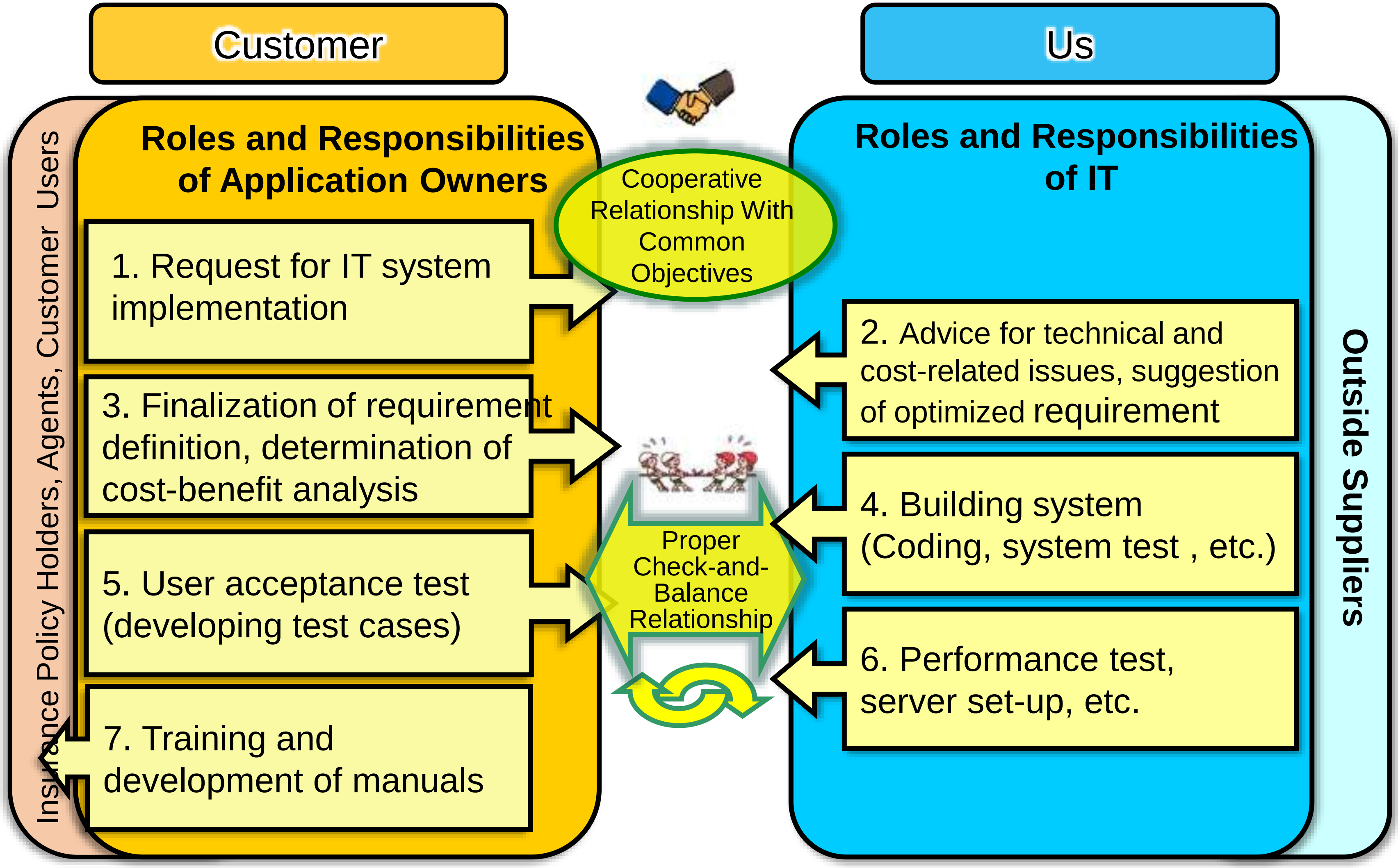
Tokio Marine Group – Stakeholder Needs Change

Start with Systems Development and Operation Company
From Programming and Systems Operation

Extend Business Domain
to Upstream Development and Management Processes

Equal Partnership between IT (Us) and Business (Customer)
(Application Owner System)

Tokio Marine Group's Application Owner System



Customer

Us

Insurance Policy Holders, Agents, Customer, Users

Roles and Responsibilities of Application Owners

1. Request for IT system implementation

3. Finalization of requirement definition, determination of cost-benefit analysis

5. User acceptance test (developing test cases)

7. Training and development of manuals

Cooperative Relationship With Common Objectives

Proper Check-and-Balance Relationship

Roles and Responsibilities of IT

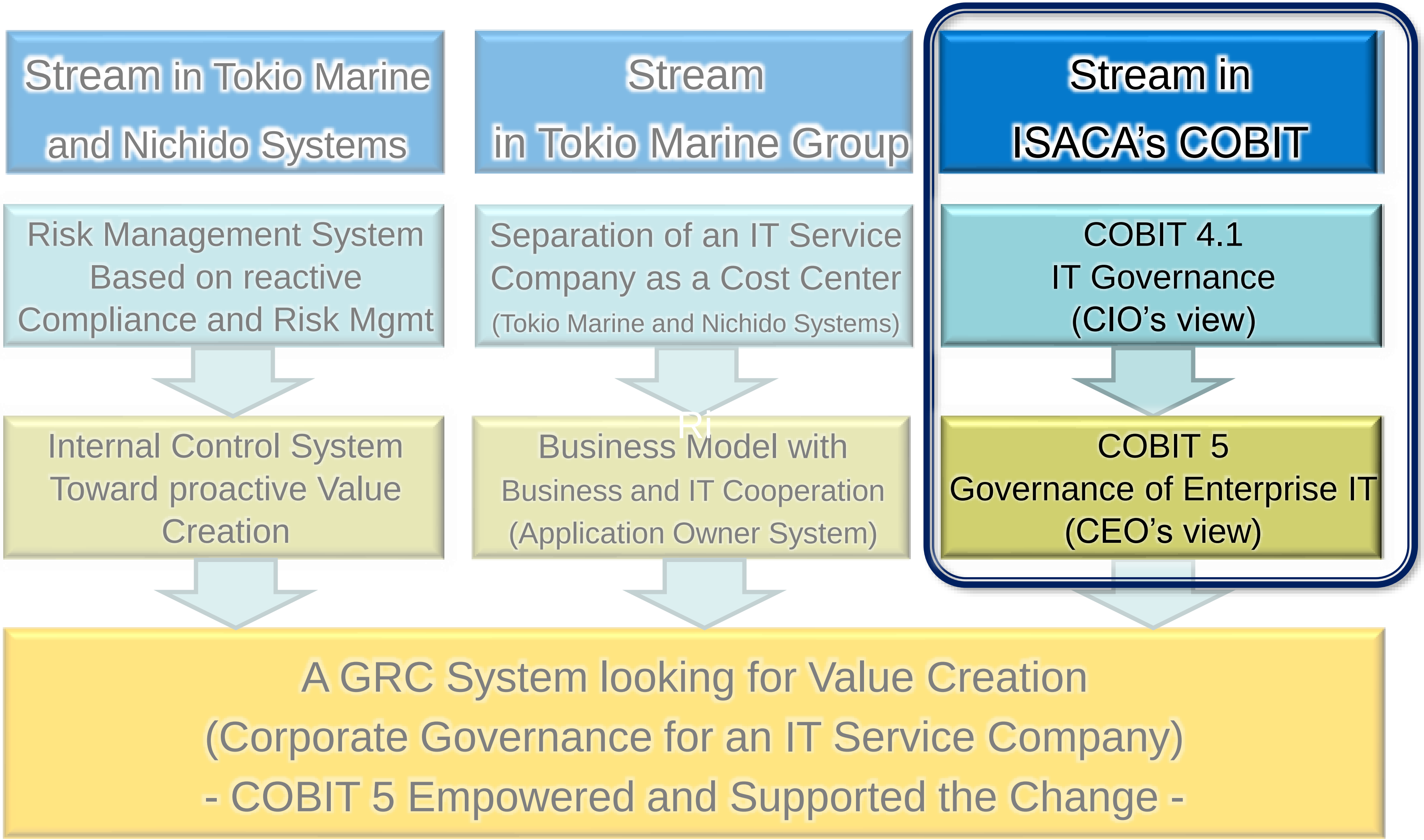
2. Advice for technical and cost-related issues, suggestion of optimized requirement

4. Building system (Coding, system test , etc.)

6. Performance test, server set-up, etc.

Outside Suppliers

Streams toward the GRC system for Value Creation



Stream in Tokio Marine and Nichido Systems

Risk Management System
Based on reactive
Compliance and Risk Mgmt

Internal Control System
Toward proactive Value
Creation

Stream in Tokio Marine Group

Separation of an IT Service
Company as a Cost Center
(Tokio Marine and Nichido Systems)

Business Model with
Business and IT Cooperation
(Application Owner System)

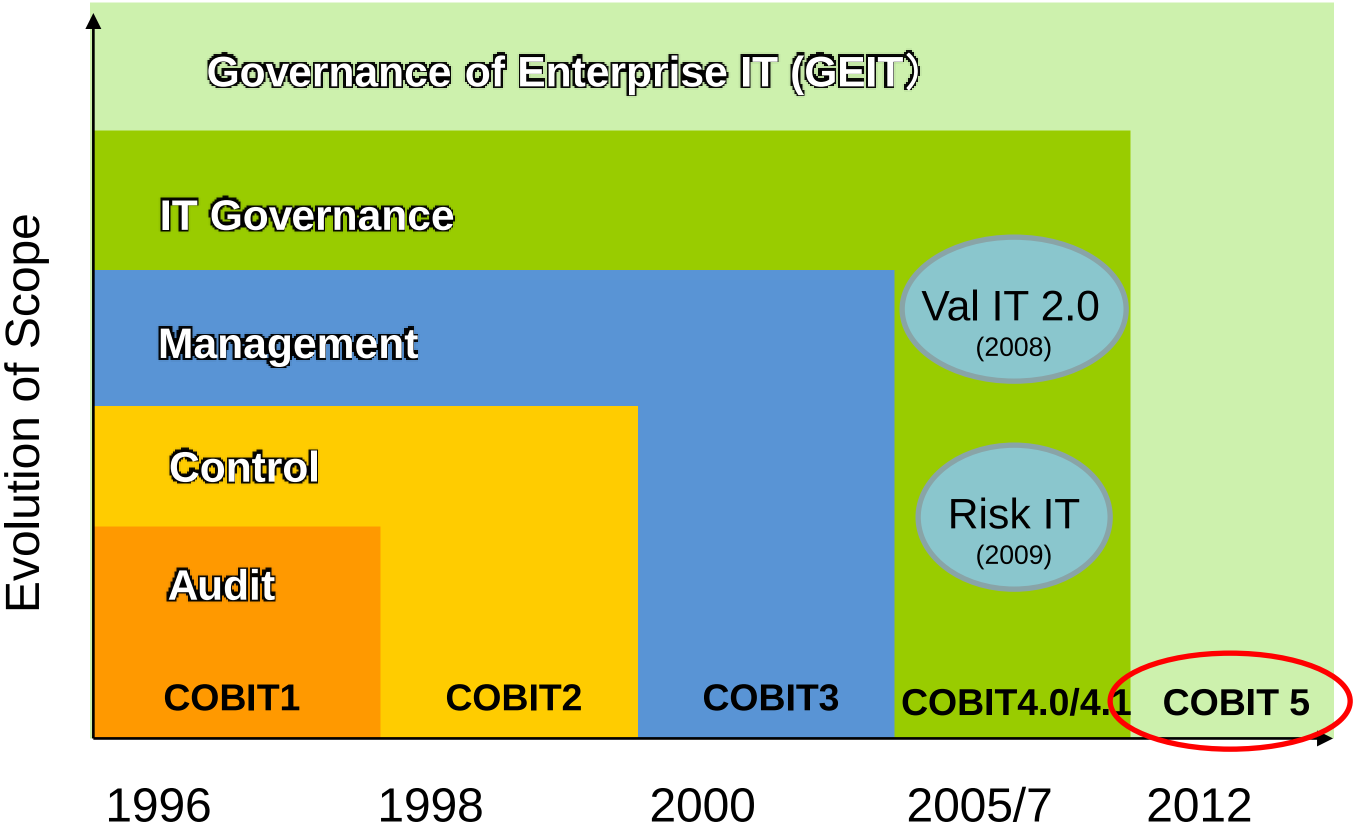
Stream in ISACA's COBIT

COBIT 4.1
IT Governance
(CIO's view)

COBIT 5
Governance of Enterprise IT
(CEO's view)

A GRC System looking for Value Creation
(Corporate Governance for an IT Service Company)
- COBIT 5 Empowered and Supported the Change -

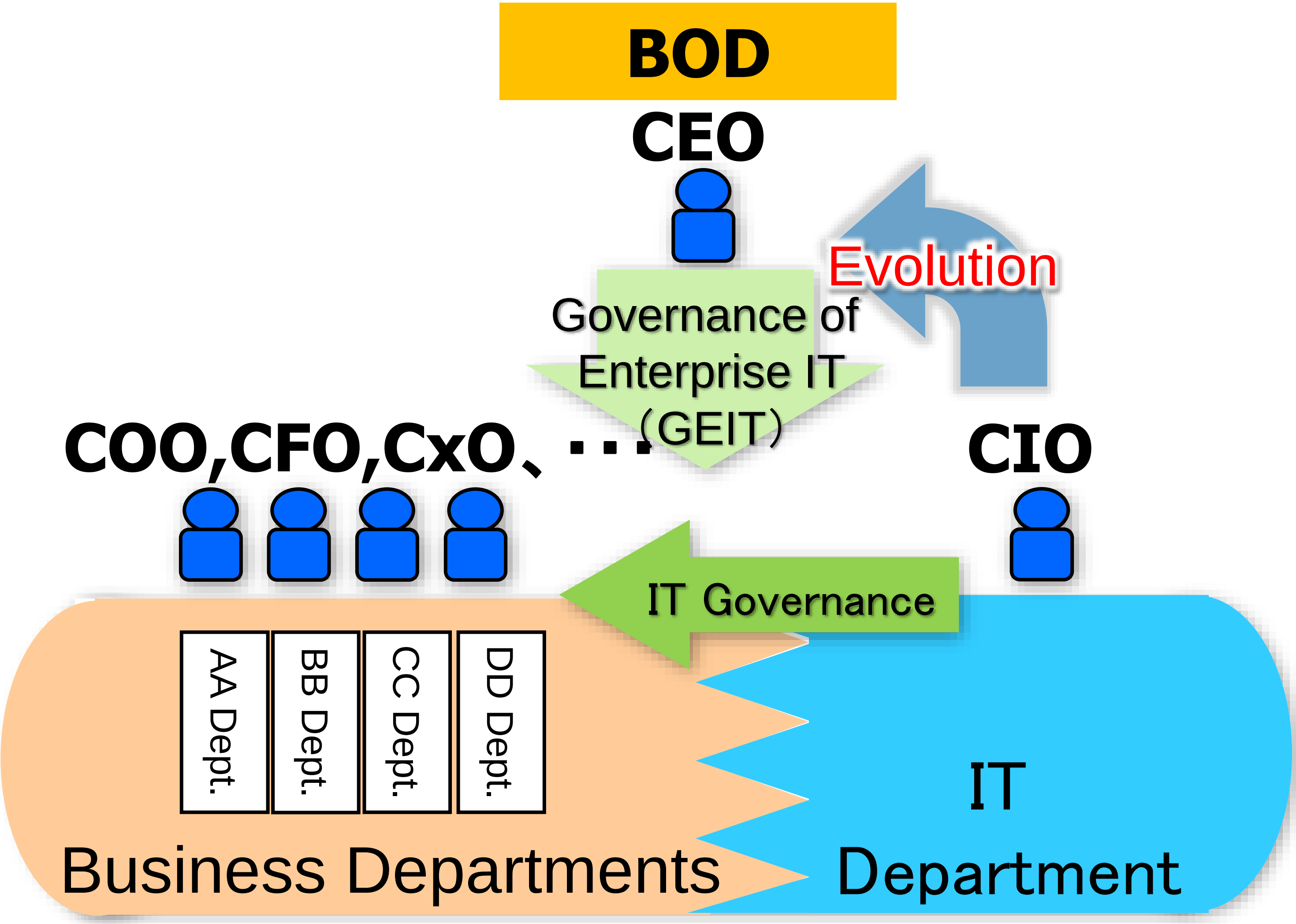
COBIT 5 – From IT Governance to GEIT


Governance of Enterprise IT (GEIT)
IT Governance
Management
Control
Audit
Val IT 2.0
(2008)
Risk IT
(2009)
Evolution of Scope
COBIT1
COBIT2
COBIT3
COBIT4.0/4.1
COBIT 5
1996
1998
2000
2005/7
2012

An business framework from ISACA, at www.isaca.org/cobit

© 2012 ISACA® All rights reserved.

Governance of Enterprise IT – Toward CEO's View



BOD

CEO

Evolution

Governance of Enterprise IT (GEIT)

COO,CFO,CxO、・・・

CIO

IT Governance

AA Dept.

BB Dept.

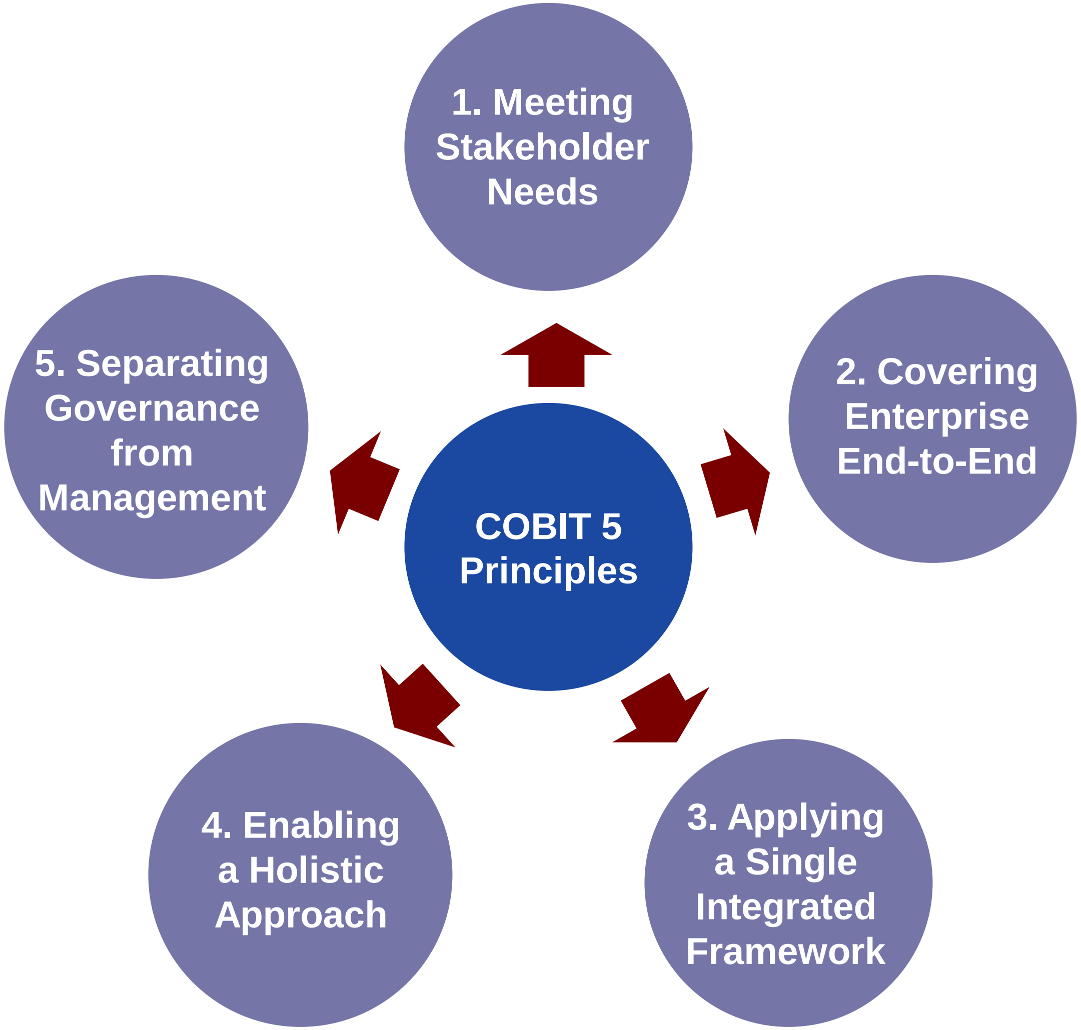
CC Dept.

DD Dept.

Business Departments

IT Department

5 Principles of COBIT 5 – Governance of Enterprise IT


1. Meeting Stakeholder Needs
5. Separating Governance from Management
COBIT 5 Principles
2. Covering Enterprise End-to-End
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

© 2012 ISACA® All rights reserved.

COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI010** Manage Configuration

Deliver, Service and Support

- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

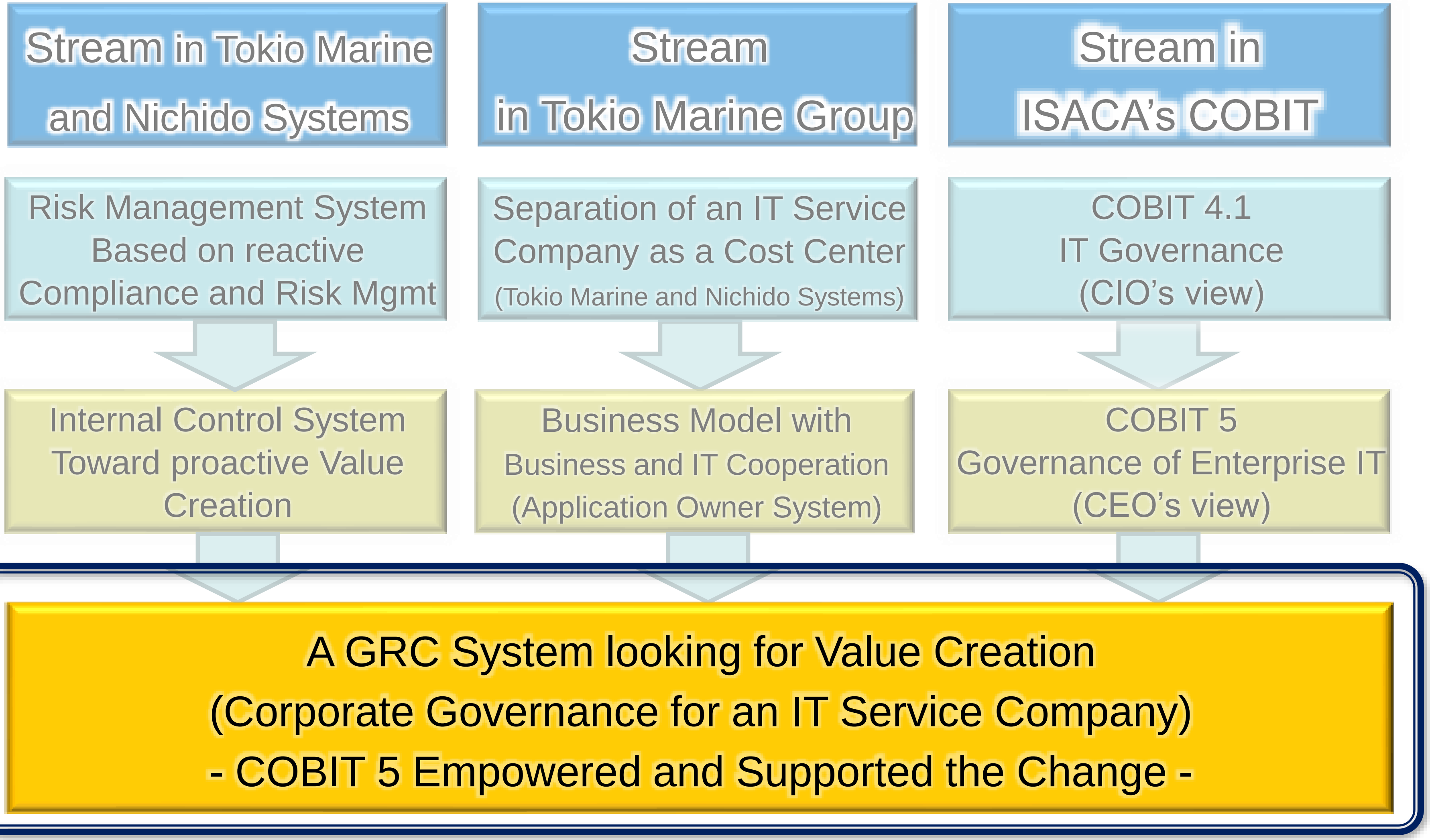
Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

© 2012 ISACA® All rights reserved.

Streams toward the GRC system for Value Creation



Stream in Tokio Marine and Nichido Systems

Risk Management System Based on reactive Compliance and Risk Mgmt

Internal Control System Toward proactive Value Creation

Stream in Tokio Marine Group

Separation of an IT Service Company as a Cost Center
(Tokio Marine and Nichido Systems)

Business Model with Business and IT Cooperation
(Application Owner System)

Stream in ISACA's COBIT

COBIT 4.1
IT Governance
(CIO's view)

COBIT 5
Governance of Enterprise IT
(CEO's view)

A GRC System looking for Value Creation
(Corporate Governance for an IT Service Company)
- COBIT 5 Empowered and Supported the Change -

Tokio Marine and Nichido Systems
Executive Management Desire

Compliance and Risk Management is very Important

But, Those without Challenge will Hurt the Company Future

Missions for a Company should be Value Creation

To do so, Steering by Management is Essential

Tokio Marine and Nichido Systems
Executive Management Desire

When Smartphones are emerging in the world,
Management will say …

Do not use it because it is very dangerous for information leakage risk

Make Maximum Use of it with appropriate Risk Controls for Value Creation

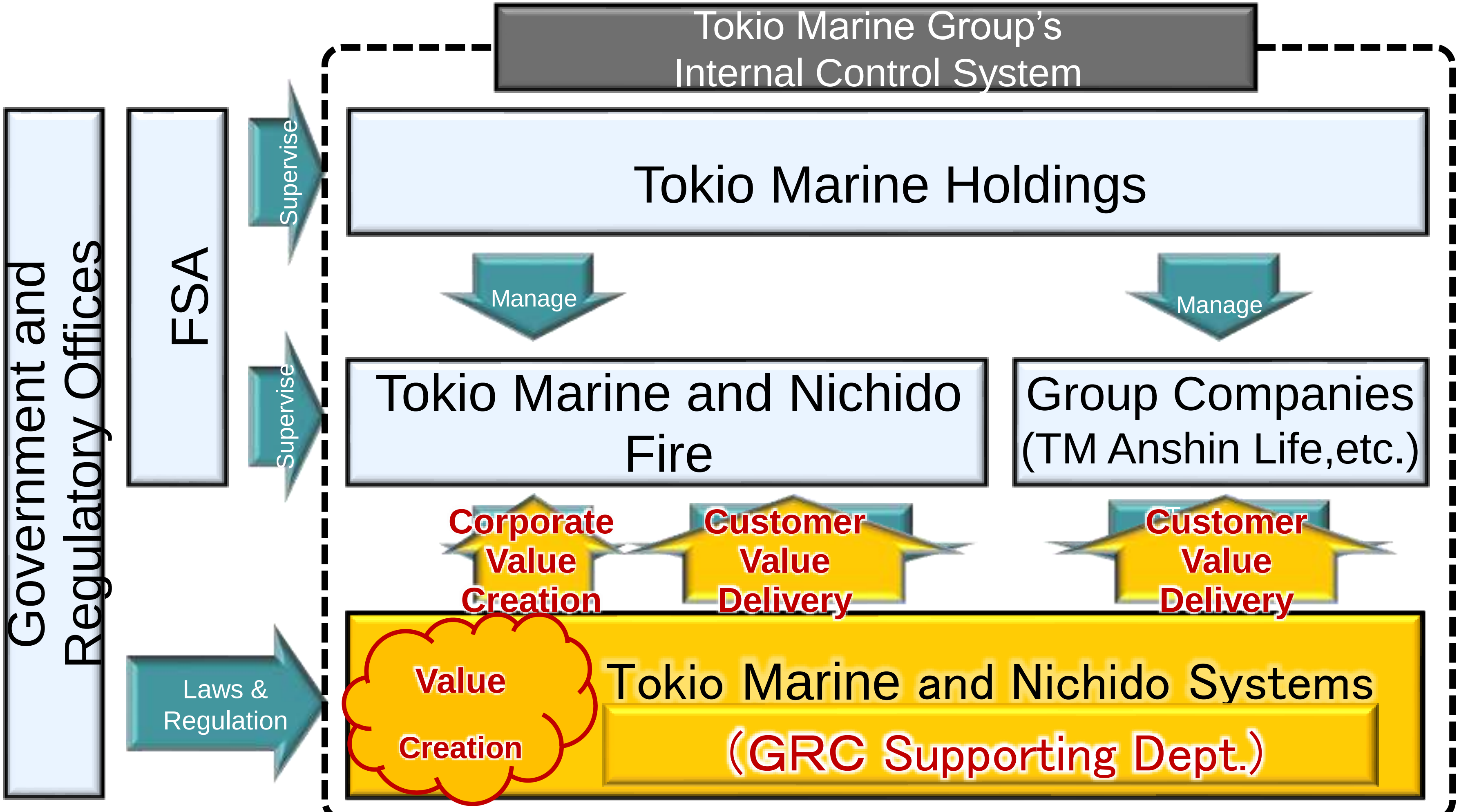
Management Desire to Reality - GRC

- ✓ Based on the Corporate Concept “We deliver the Technology with our whole heart, Globally,” Management is Steering the Company.
- ✓ We Visualized it by using the term, “GRC”.

(G) Governance Objective: Create Value
(R) Risk Management Objective: Optimize Risk
(C) Compliance Objective: Keep Rules

By using Tokio Marine Group’s Internal Control Framework, “G”, “R” and “C” are handled effectively and efficiently with integrated manner.

The Environment Around Us



Government and Regulatory Offices

FSA

Supervise

Supervise

Laws & Regulation

Tokio Marine Group's Internal Control System

Tokio Marine Holdings

Manage

Manage

Tokio Marine and Nichido Fire

Group Companies (TM Anshin Life,etc.)

Corporate Value Creation

Customer Value Delivery

Customer Value Delivery

Value Creation

Tokio Marine and Nichido Systems

（GRC Supporting Dept.）

Today’s Contents

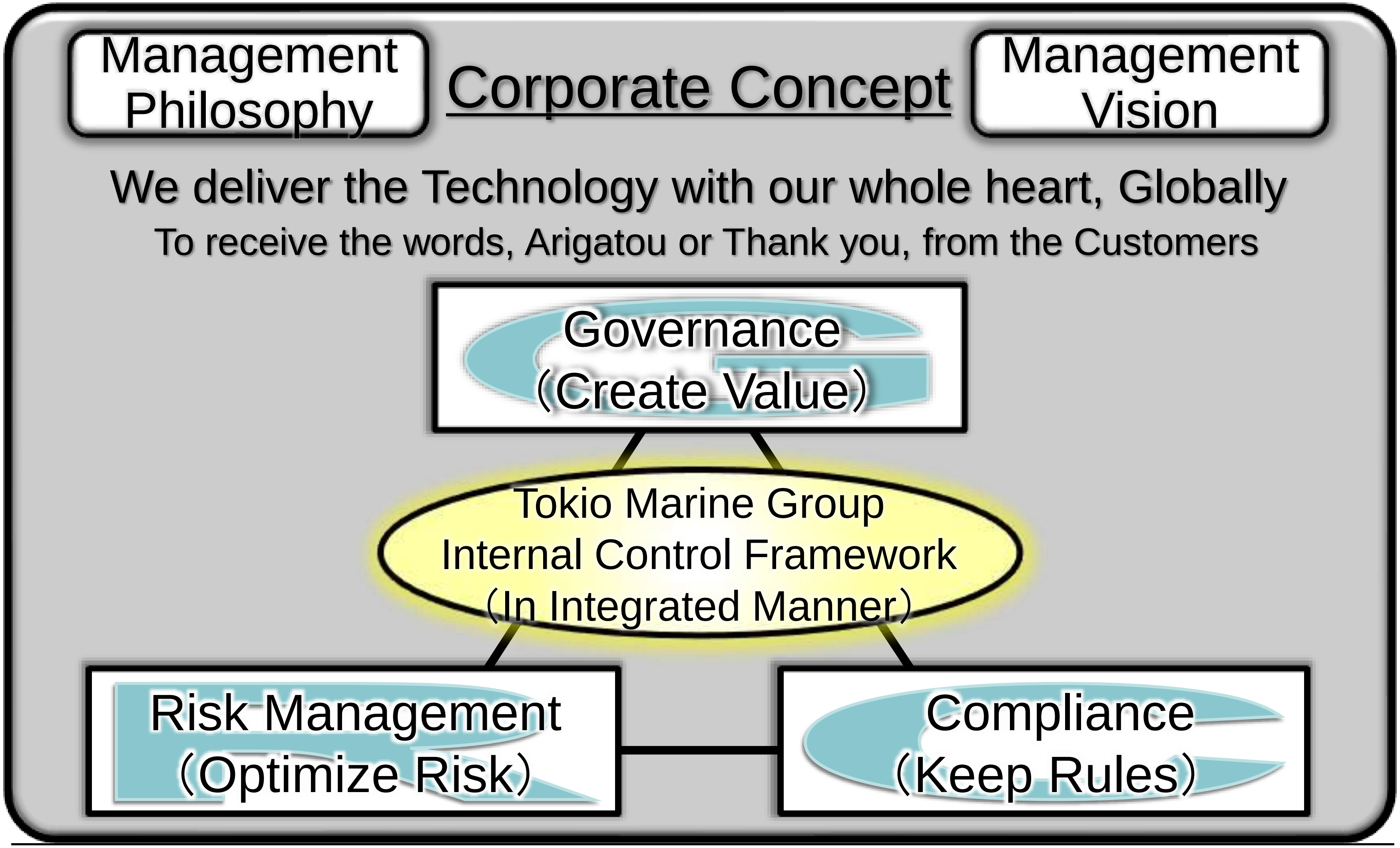
1. Introduction - Myself and My Company

2. From Reactive Internal Control to Proactive GRC

3. GRC at Tokio Marine and Nichido Systems

4. COBIT 5 Empowered and Supported the Change

Definition of GRC Concept



Management Philosophy

Corporate Concept

Management Vision

We deliver the Technology with our whole heart, Globally

To receive the words, Arigatou or Thank you, from the Customers

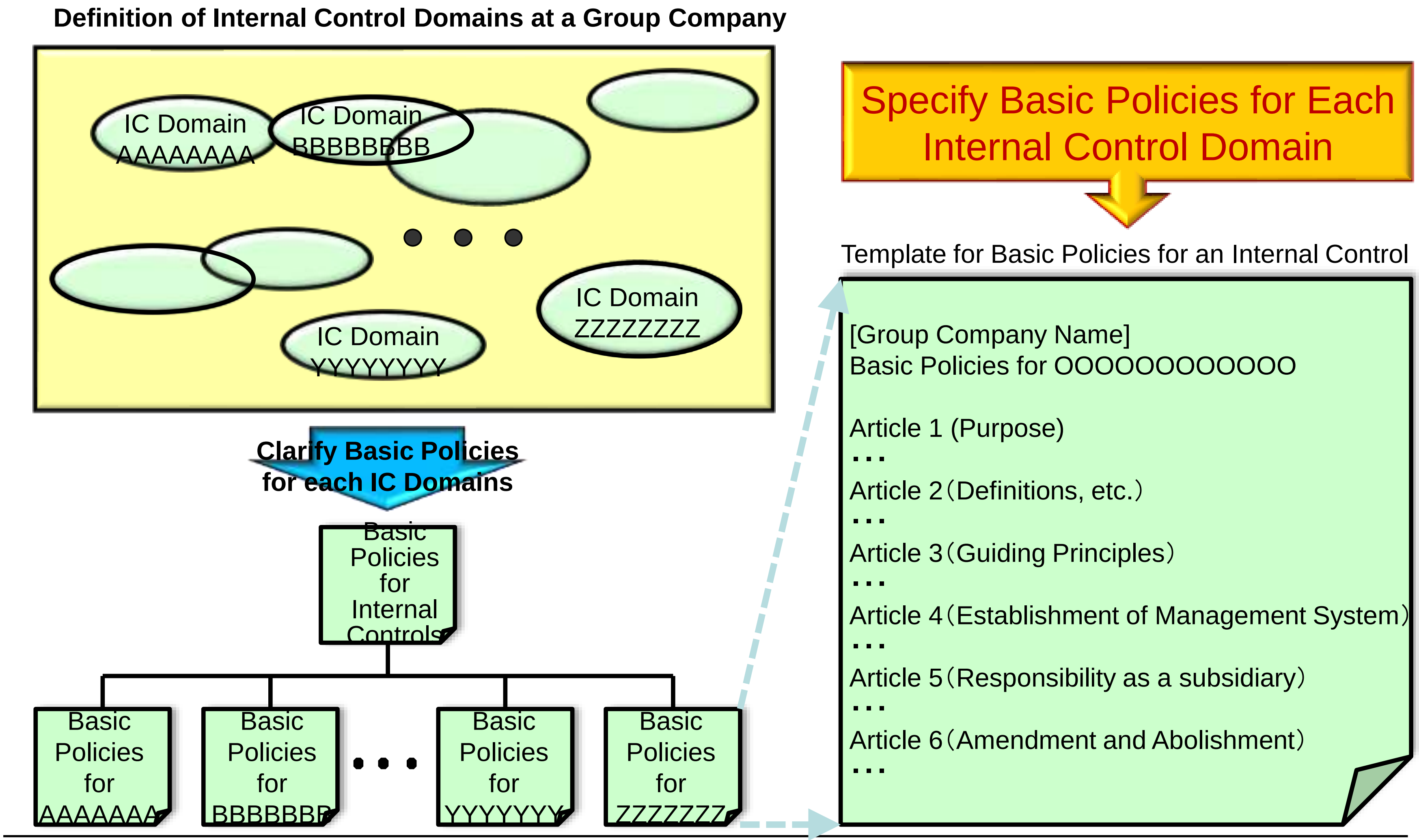
Governance
（Create Value）

Tokio Marine Group
Internal Control Framework
（In Integrated Manner）

Risk Management
（Optimize Risk）

Compliance
（Keep Rules）

Internal Control Framework at Tokio Marine Group



Definition of Internal Control Domains at a Group Company

IC Domain AAAAAAAA
IC Domain BBBBBBBB
IC Domain YYYYYYYY
IC Domain ZZZZZZZZ
● ● ●
Clarify Basic Policies for each IC Domains
Basic Policies for Internal Controls
Basic Policies for AAAAAAA
Basic Policies for BBBBBBB
• • •
Basic Policies for YYYYYYY
Basic Policies for ZZZZZZZ

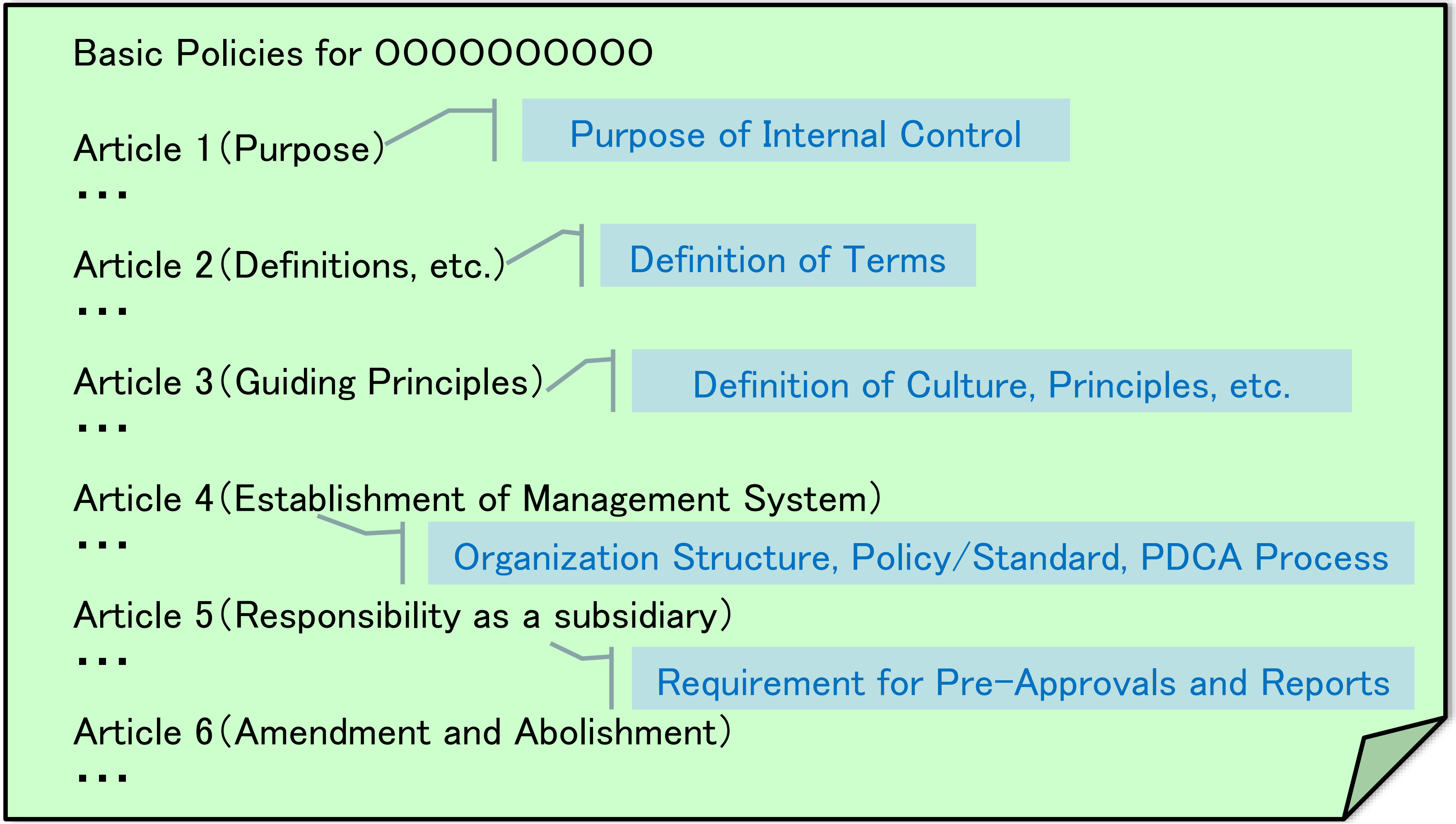
Specify Basic Policies for Each Internal Control Domain

Template for Basic Policies for an Internal Control

[Group Company Name]
Basic Policies for OOOOOOOOOOOO

Article 1 (Purpose)
・・・
Article 2（Definitions, etc.）
・・・
Article 3（Guiding Principles）
・・・
Article 4（Establishment of Management System）
・・・
Article 5（Responsibility as a subsidiary）
・・・
Article 6（Amendment and Abolishment）
・・・

Internal Control Goal Definitions in Basic Policies



Basic Policies for OOOOOOOOOO

Article 1（Purpose）

・・・

Purpose of Internal Control

Article 2（Definitions, etc.）

・・・

Definition of Terms

Article 3（Guiding Principles）

・・・

Definition of Culture, Principles, etc.

Article 4（Establishment of Management System）

・・・

Organization Structure, Policy/Standard, PDCA Process

Article 5（Responsibility as a subsidiary）

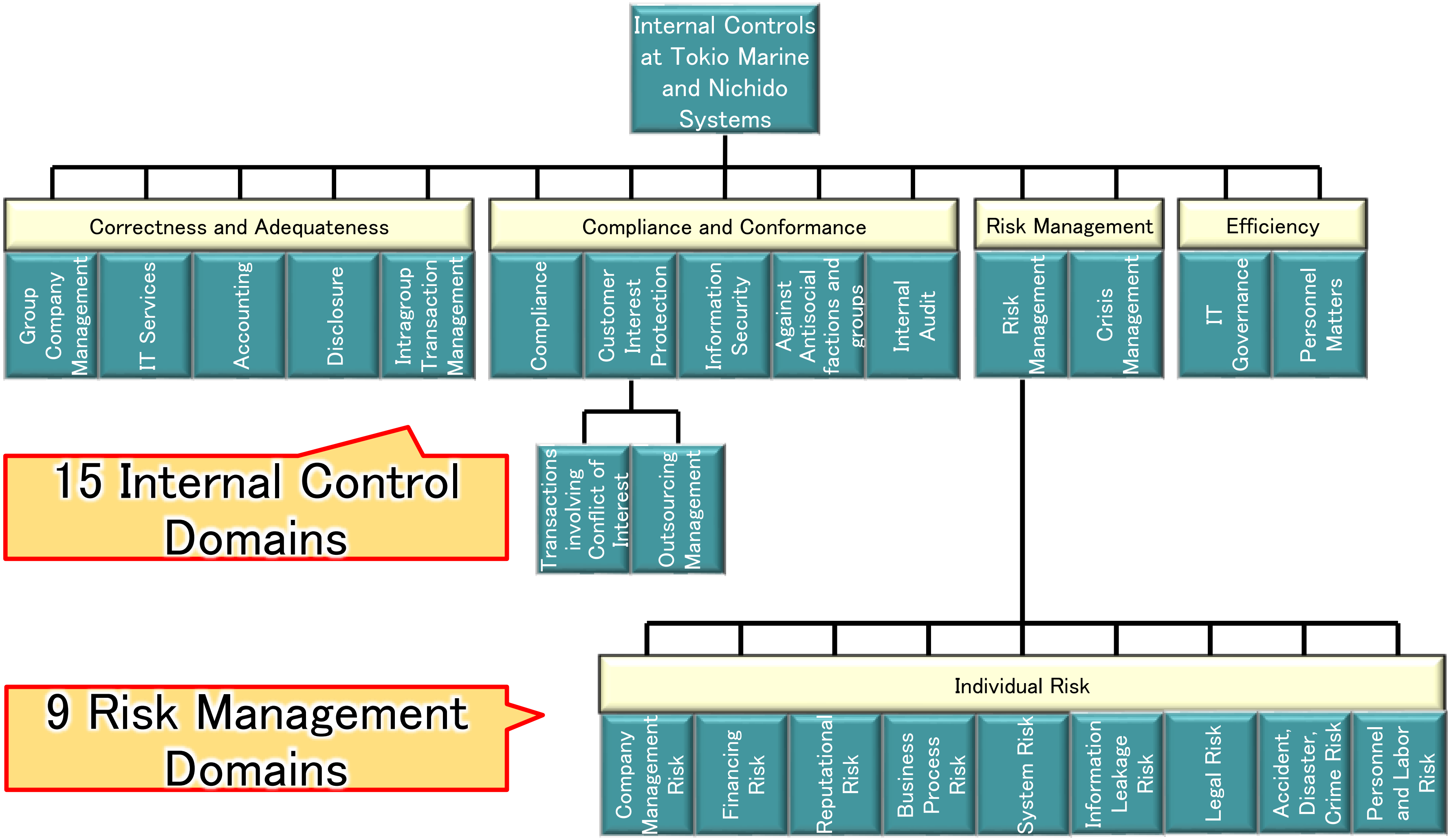
・・・

Requirement for Pre-Approvals and Reports

Article 6（Amendment and Abolishment）

・・・

Internal Control Domains
at Tokio Marine and Nichido Systems



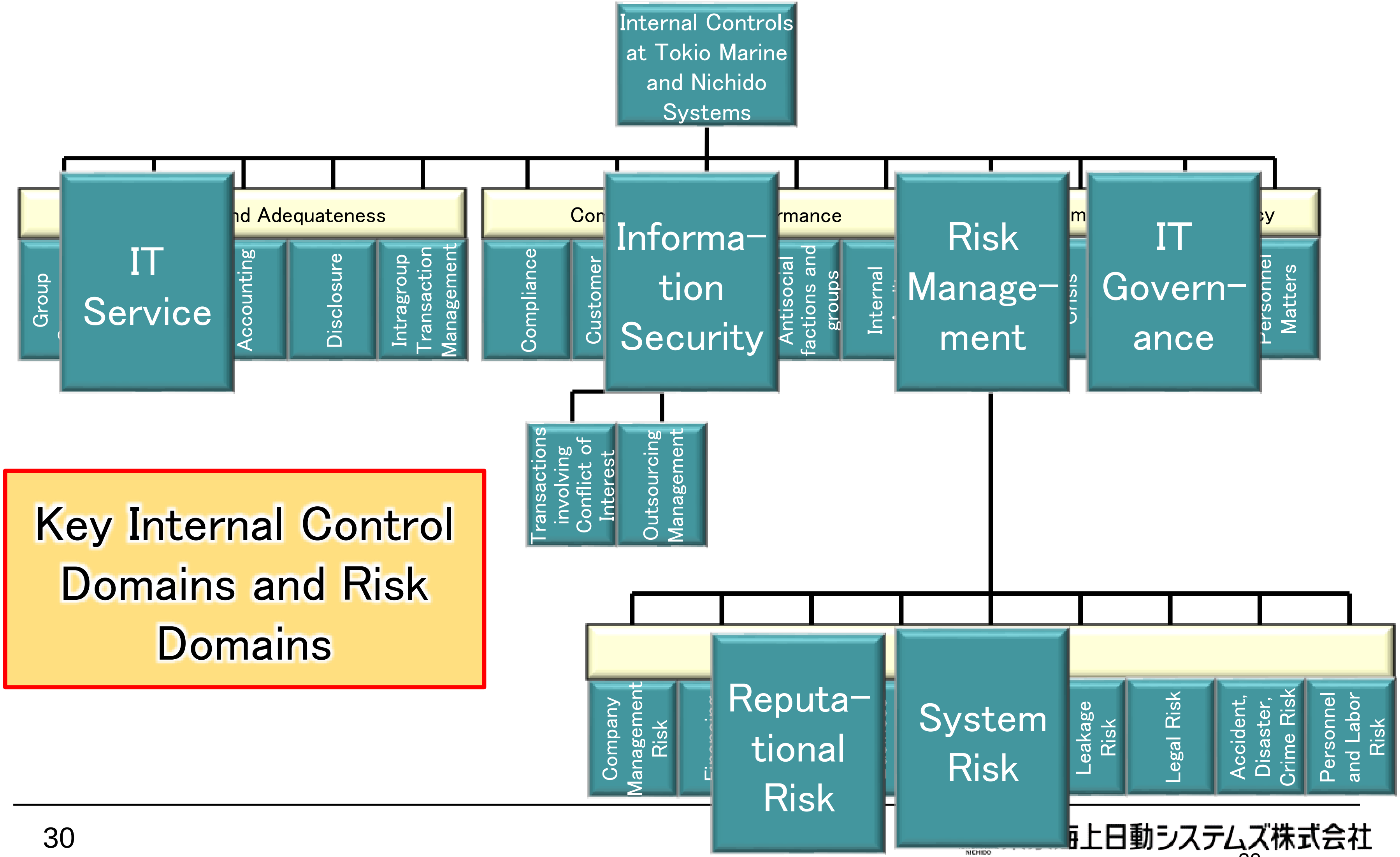
Internal Controls at Tokio Marine and Nichido Systems

- Correctness and Adequateness
  - Group Company Management
  - IT Services
  - Accounting
  - Disclosure
  - Intragroup Transaction Management
- Compliance and Conformance
  - Compliance
  - Customer Interest Protection
    - Transactions involving Conflict of Interest
    - Outsourcing Management
  - Information Security
  - Against Antisocial factions and groups
  - Internal Audit
- Risk Management
  - Risk Management
    - Individual Risk
      - Company Management Risk
      - Financing Risk
      - Reputational Risk
      - Business Process Risk
      - System Risk
      - Information Leakage Risk
      - Legal Risk
      - Accident, Disaster, Crime Risk
      - Personnel and Labor Risk
  - Crisis Management
- Efficiency
  - IT Governance
  - Personnel Matters

15 Internal Control Domains

9 Risk Management Domains

Internal Control Domains at Tokio Marine and Nichido Systems


Internal Controls at Tokio Marine and Nichido Systems

Group

IT Service

nd Adequateness

Accounting

Disclosure

Intragroup Transaction Management

Con

Compliance

Customer

Information Security

rmance

Antisocial factions and groups

Internal

Risk Management

IT Governance

cy

Personnel Matters

Transactions involving Conflict of Interest

Outsourcing Management

Company Management Risk

Reputational Risk

System Risk

Leakage Risk

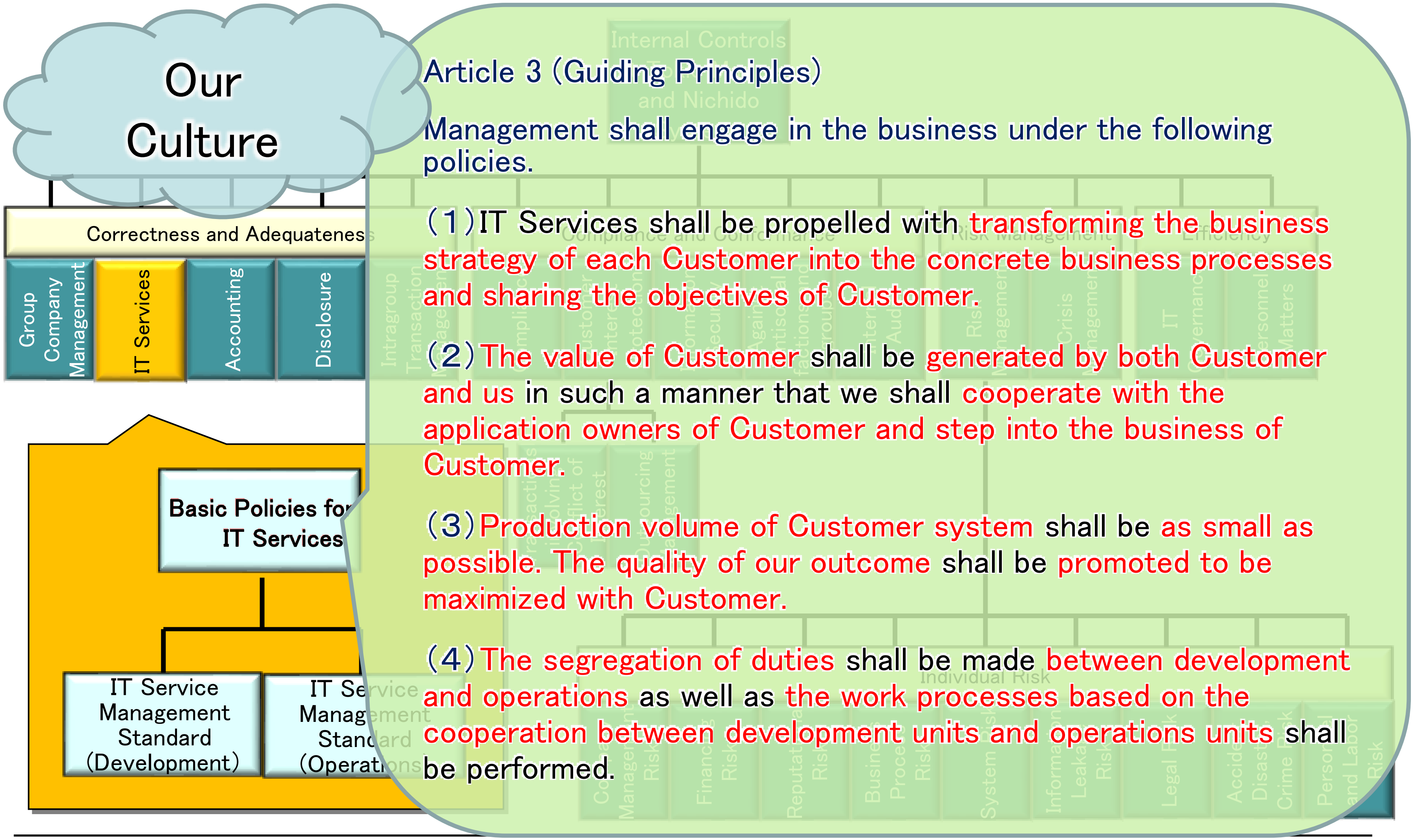
Legal Risk

Accident, Disaster, Crime Risk

Personnel and Labor Risk

Key Internal Control Domains and Risk Domains

Value Creating Internal Control – IT Services


Our Culture
Internal Controls
and Nichido
Correctness and Adequateness
Compliance and Conformance
Risk Management
Efficiency
Group Company Management
IT Services
Accounting
Disclosure
Intragroup Transaction
Crisis Management
IT Governance
Personnel Matters
Basic Policies for IT Services
IT Service Management Standard (Development)
IT Service Management Standard (Operations)
Individual Risk
Financial Risk
Reputational Risk
Business Process Risk
System Risk
Information Leakage Risk
Legal Risk
Accident Disaster Crime
Personnel and Labor Risk

Article 3 (Guiding Principles)

Management shall engage in the business under the following policies.

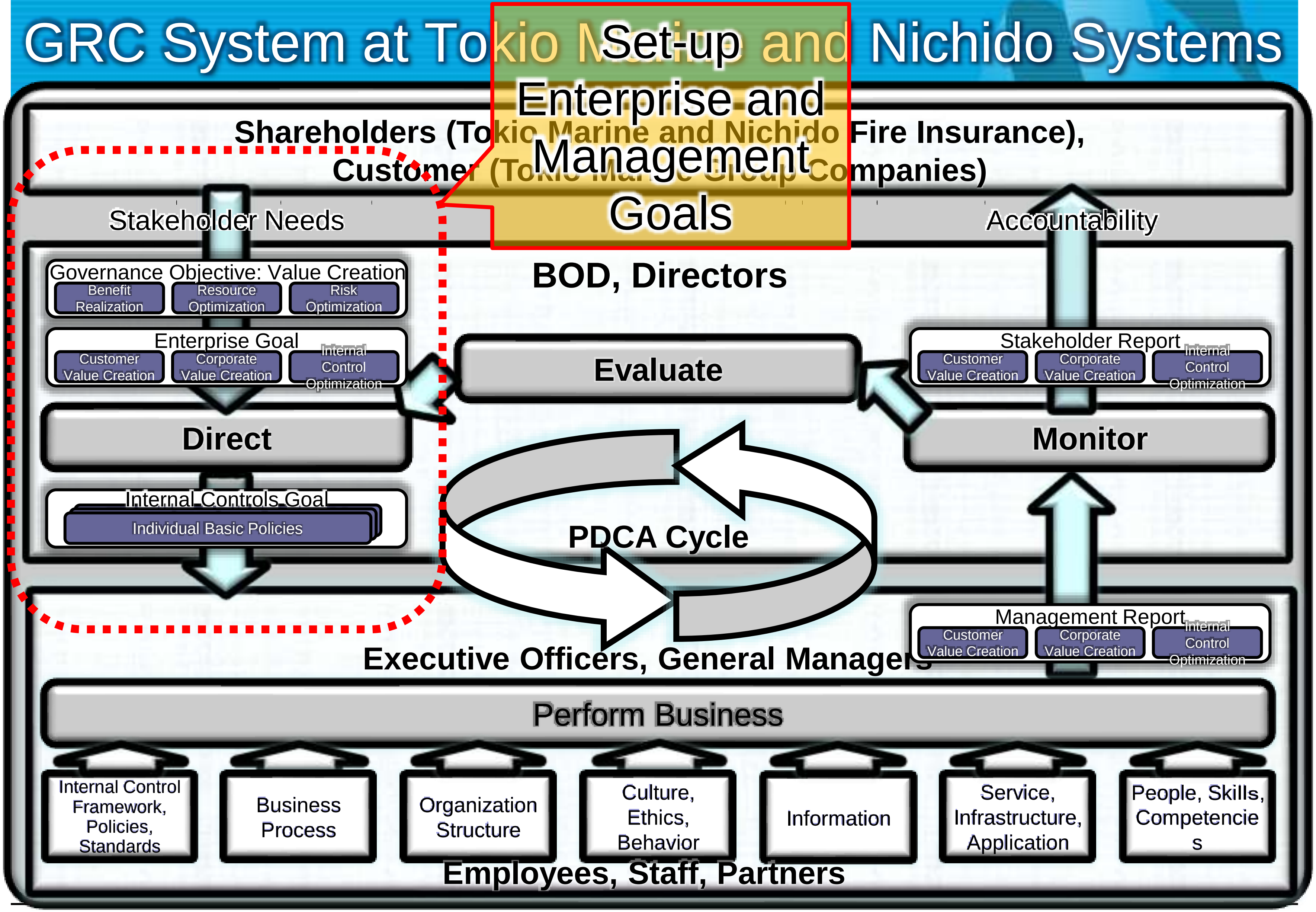
（1）IT Services shall be propelled with transforming the business strategy of each Customer into the concrete business processes and sharing the objectives of Customer.

（2）The value of Customer shall be generated by both Customer and us in such a manner that we shall cooperate with the application owners of Customer and step into the business of Customer.

（3）Production volume of Customer system shall be as small as possible. The quality of our outcome shall be promoted to be maximized with Customer.

（4）The segregation of duties shall be made between development and operations as well as the work processes based on the cooperation between development units and operations units shall be performed.

GRC System at Tokio Marine and Nichido Systems



Set-up Enterprise and Management Goals

Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)

Stakeholder Needs

Accountability

BOD, Directors

Governance Objective: Value Creation
- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goal
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Direct

Internal Controls Goal
- Individual Basic Policies

Evaluate

PDCA Cycle

Stakeholder Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Monitor

Management Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

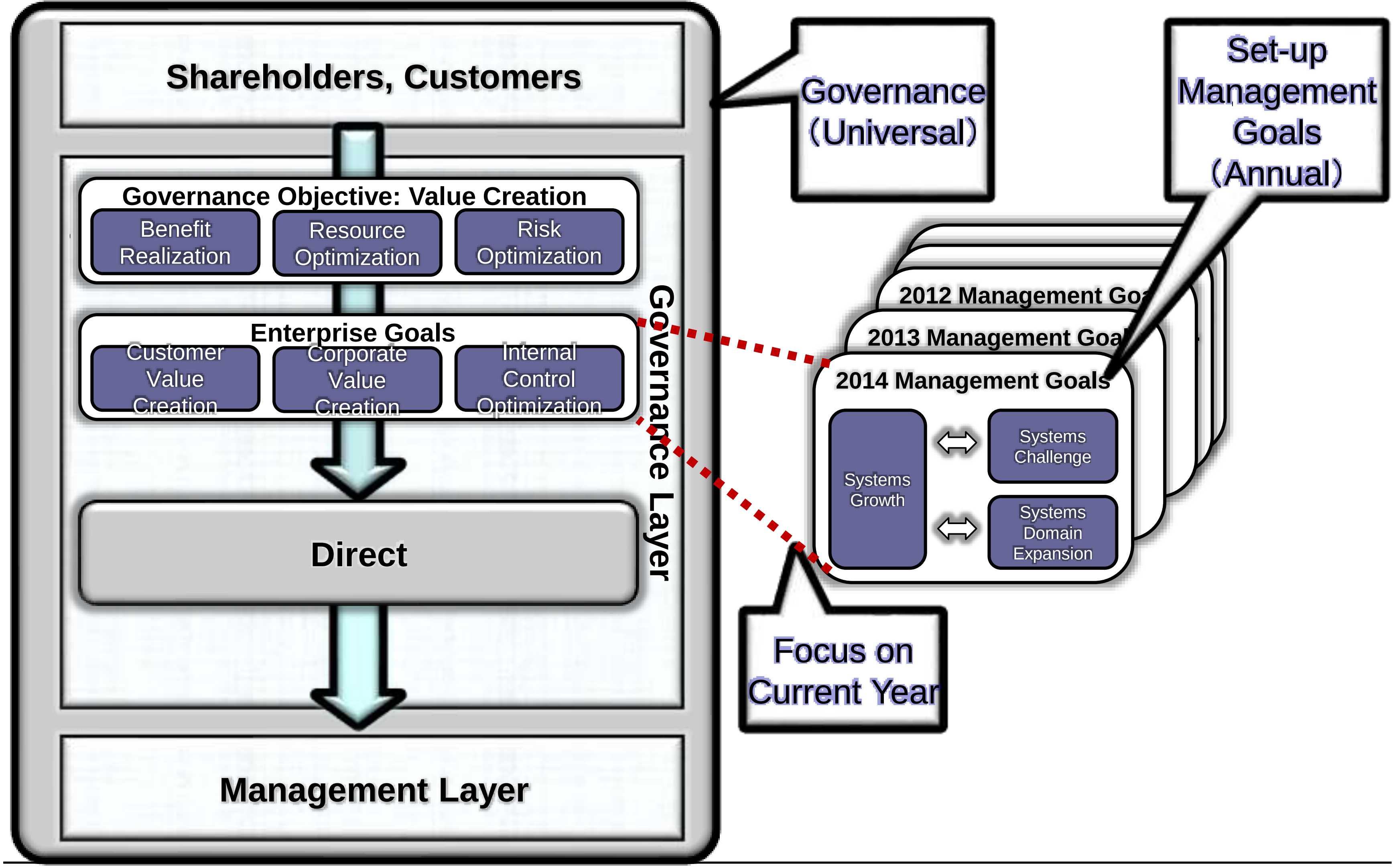
Executive Officers, General Managers

Perform Business

- Internal Control Framework, Policies, Standards
- Business Process
- Organization Structure
- Culture, Ethics, Behavior
- Information
- Service, Infrastructure, Application
- People, Skills, Competencies

Employees, Staff, Partners

Set-up Management Goals



Shareholders, Customers

Governance Objective: Value Creation

- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goals

- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Direct

Management Layer

Governance Layer

Governance (Universal)

Set-up Management Goals (Annual)

2012 Management Go

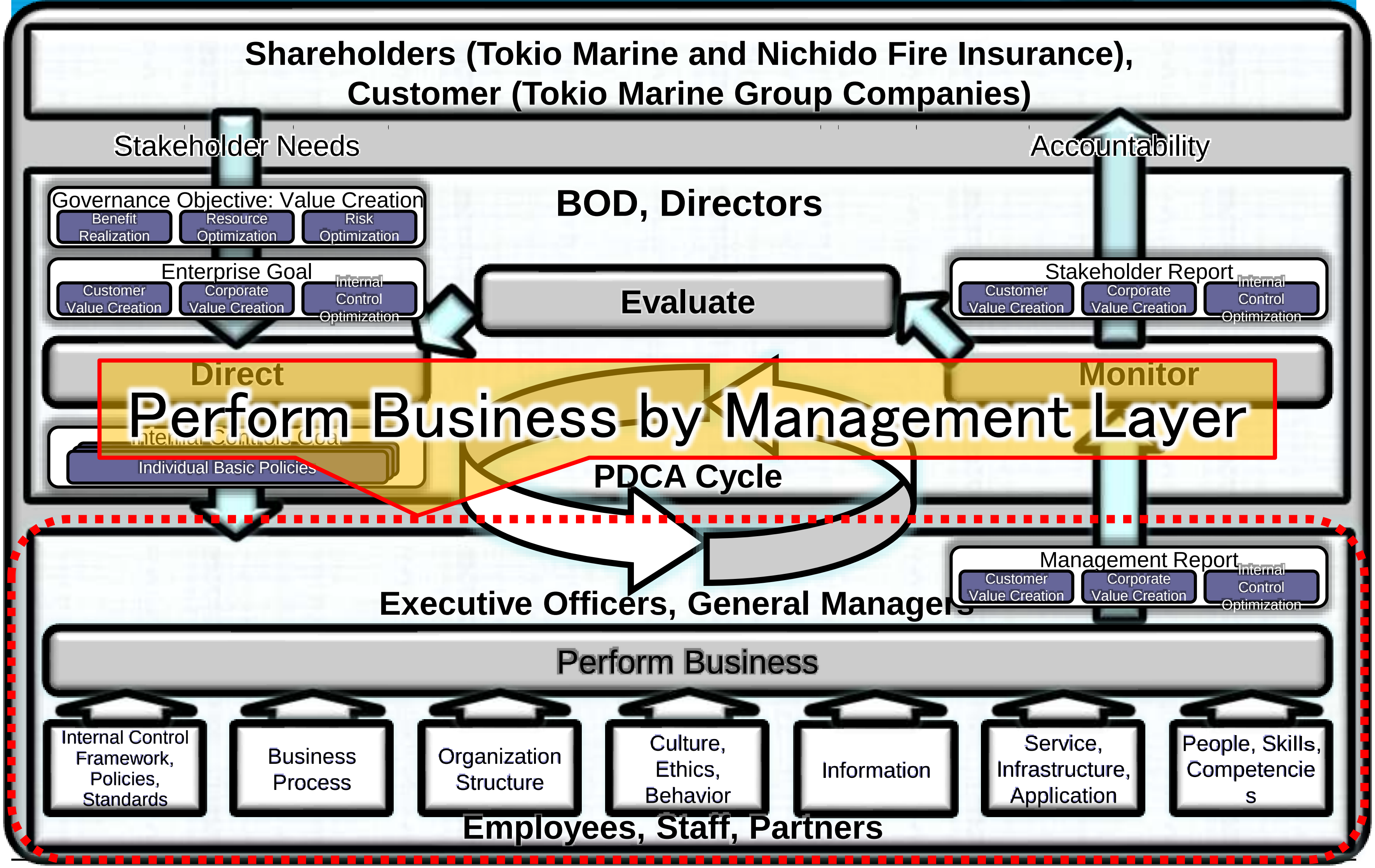
2013 Management Goa

2014 Management Goals

- Systems Growth ⇔ Systems Challenge
- Systems Growth ⇔ Systems Domain Expansion

Focus on Current Year

GRC System at Tokio Marine and Nichido Systems



Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)

Stakeholder Needs

Accountability

BOD, Directors

Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization

Enterprise Goal
Customer Value Creation
Corporate Value Creation
Internal Control Optimization

Evaluate

Stakeholder Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization

Direct

Monitor

Perform Business by Management Layer

Internal Controls Goal
Individual Basic Policies

PDCA Cycle

Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization

Executive Officers, General Managers

Perform Business

Internal Control Framework, Policies, Standards

Business Process

Organization Structure

Culture, Ethics, Behavior

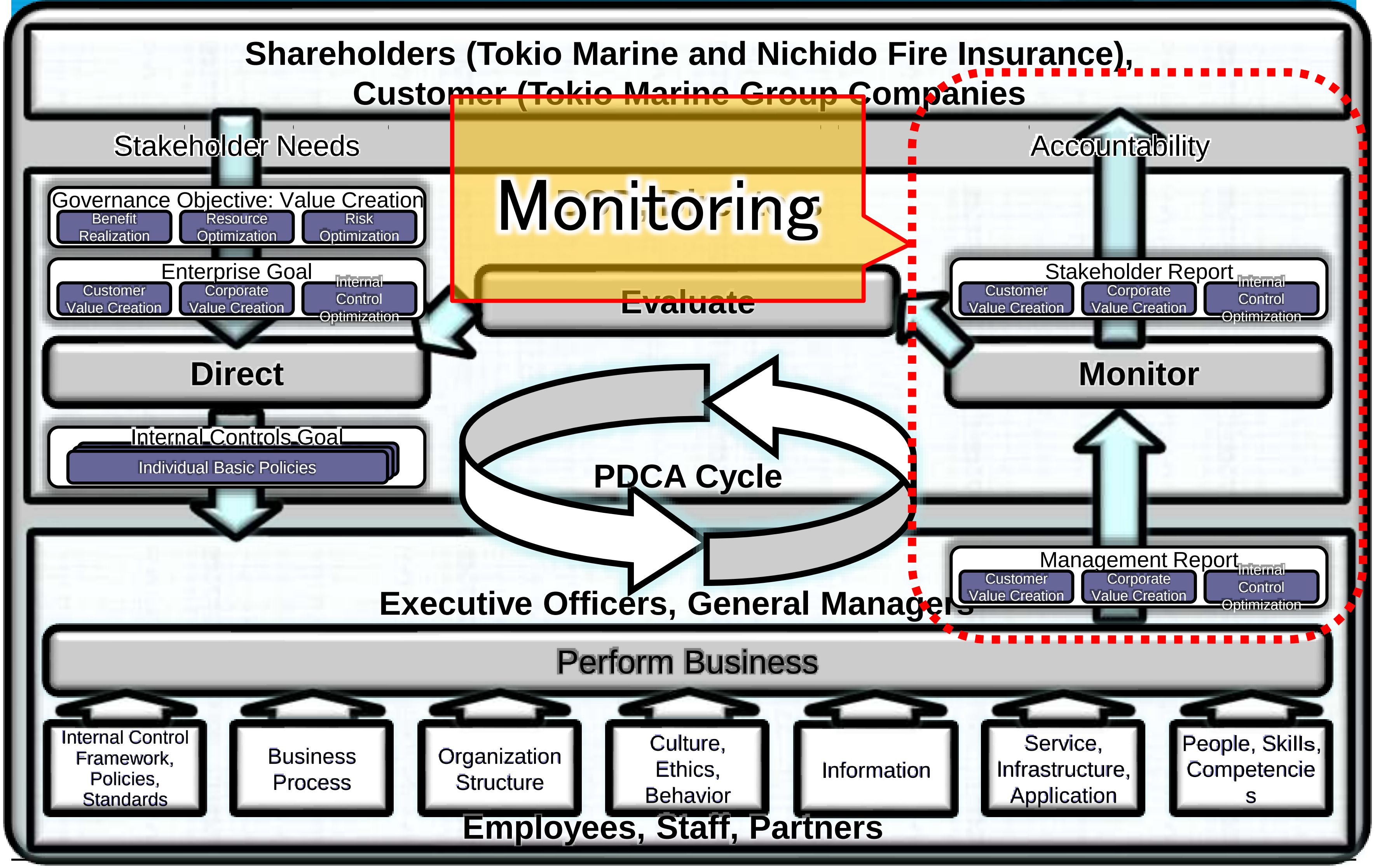
Information

Service, Infrastructure, Application

People, Skills, Competencies

Employees, Staff, Partners

GRC System at Tokio Marine and Nichido Systems



Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies

Stakeholder Needs

Accountability

Governance Objective: Value Creation
- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goal
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Direct

Internal Controls Goal
- Individual Basic Policies

Monitoring

Evaluate

PDCA Cycle

Stakeholder Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Monitor

Management Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

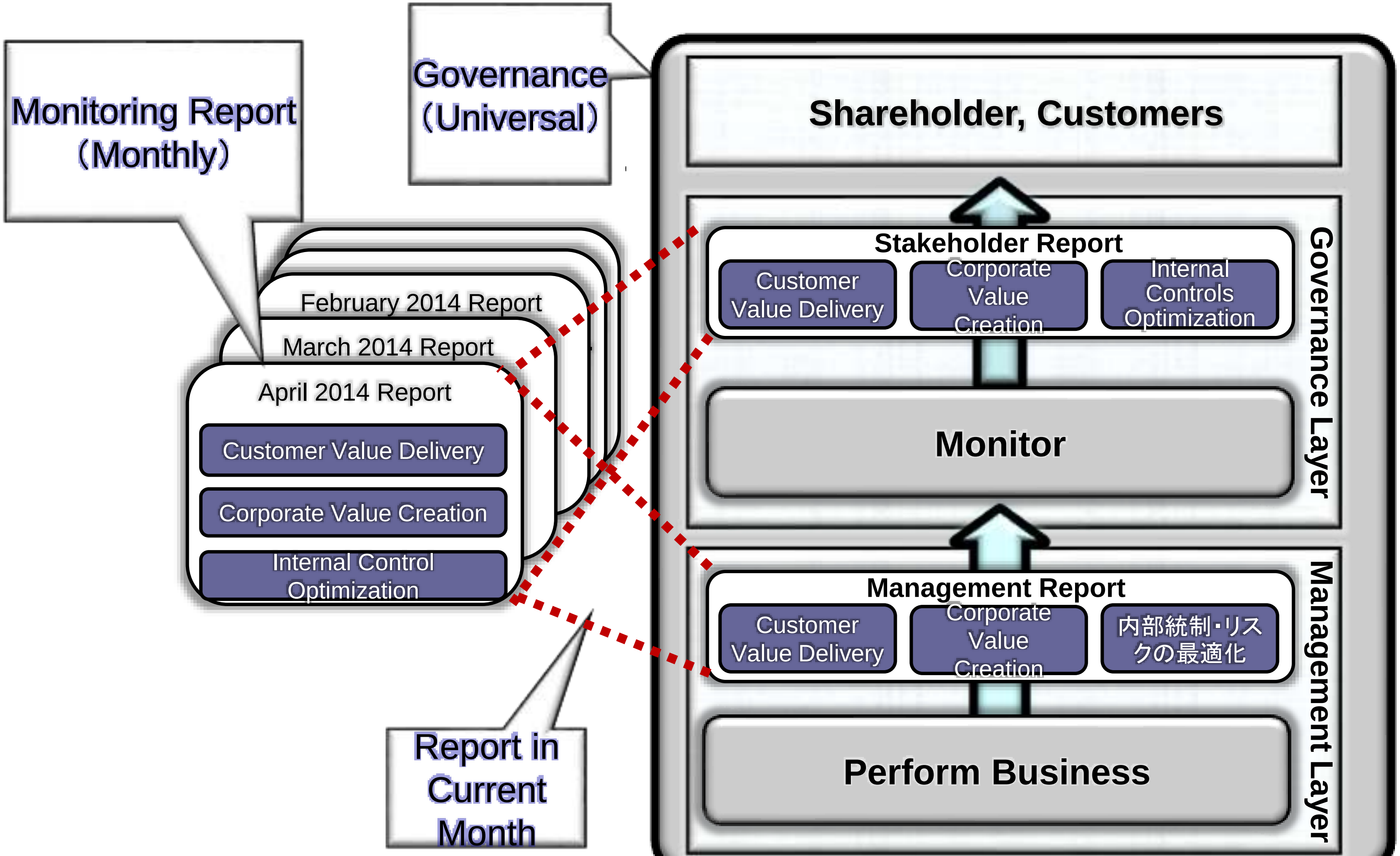
Executive Officers, General Managers

Perform Business

- Internal Control Framework, Policies, Standards
- Business Process
- Organization Structure
- Culture, Ethics, Behavior
- Information
- Service, Infrastructure, Application
- People, Skills, Competencies

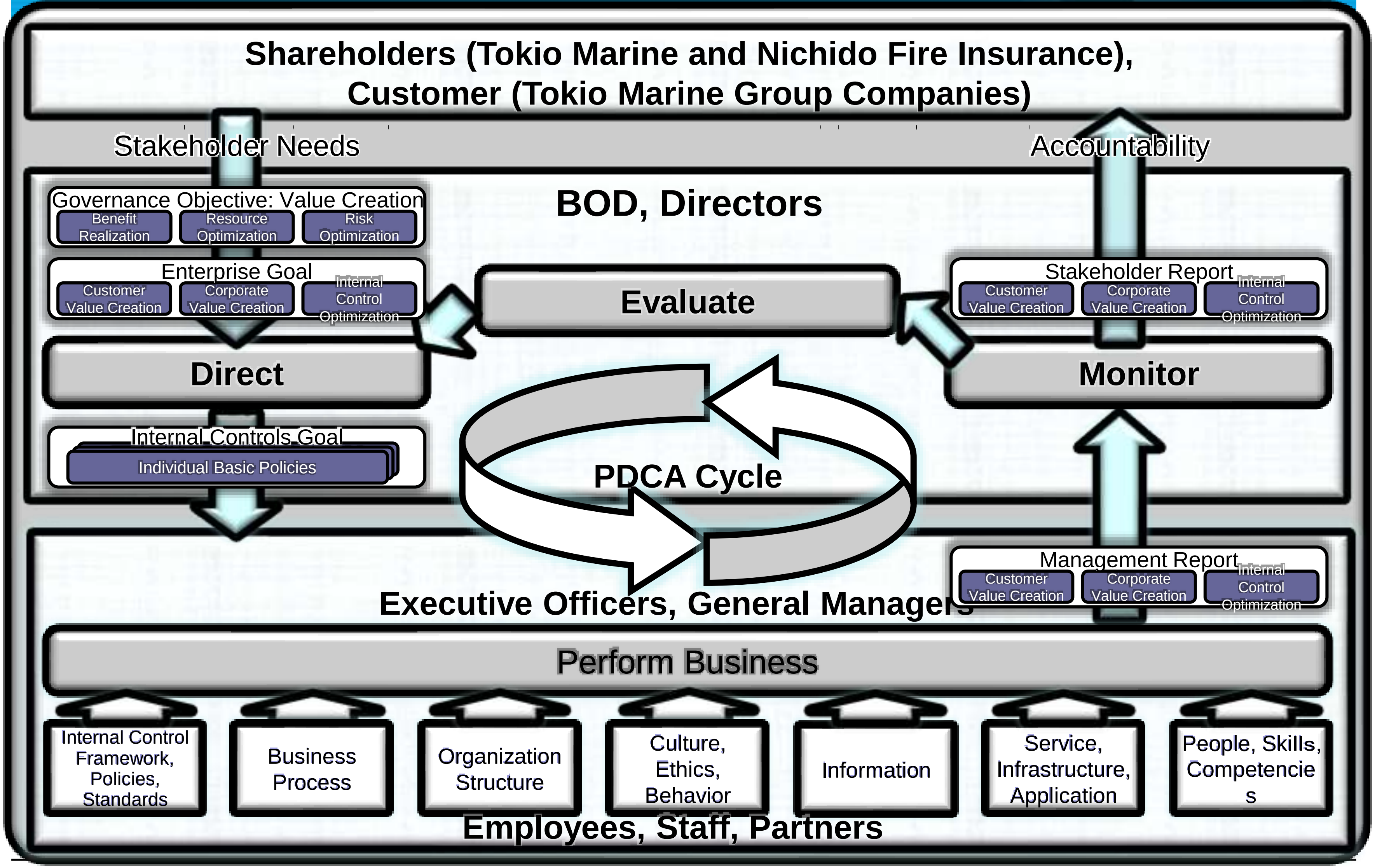
Employees, Staff, Partners

Management Report and Stakeholder Report



Monitoring Report
（Monthly）
Governance
（Universal）
February 2014 Report
March 2014 Report
April 2014 Report
Customer Value Delivery
Corporate Value Creation
Internal Control Optimization
Report in Current Month
Shareholder, Customers
Stakeholder Report
Customer Value Delivery
Corporate Value Creation
Internal Controls Optimization
Monitor
Governance Layer
Management Report
Customer Value Delivery
Corporate Value Creation
内部統制・リスクの最適化
Perform Business
Management Layer

GRC System at Tokio Marine and Nichido Systems



Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)

Stakeholder Needs

Accountability

BOD, Directors

Governance Objective: Value Creation
- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goal
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Evaluate

Stakeholder Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Direct

Monitor

Internal Controls Goal
- Individual Basic Policies

PDCA Cycle

Management Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

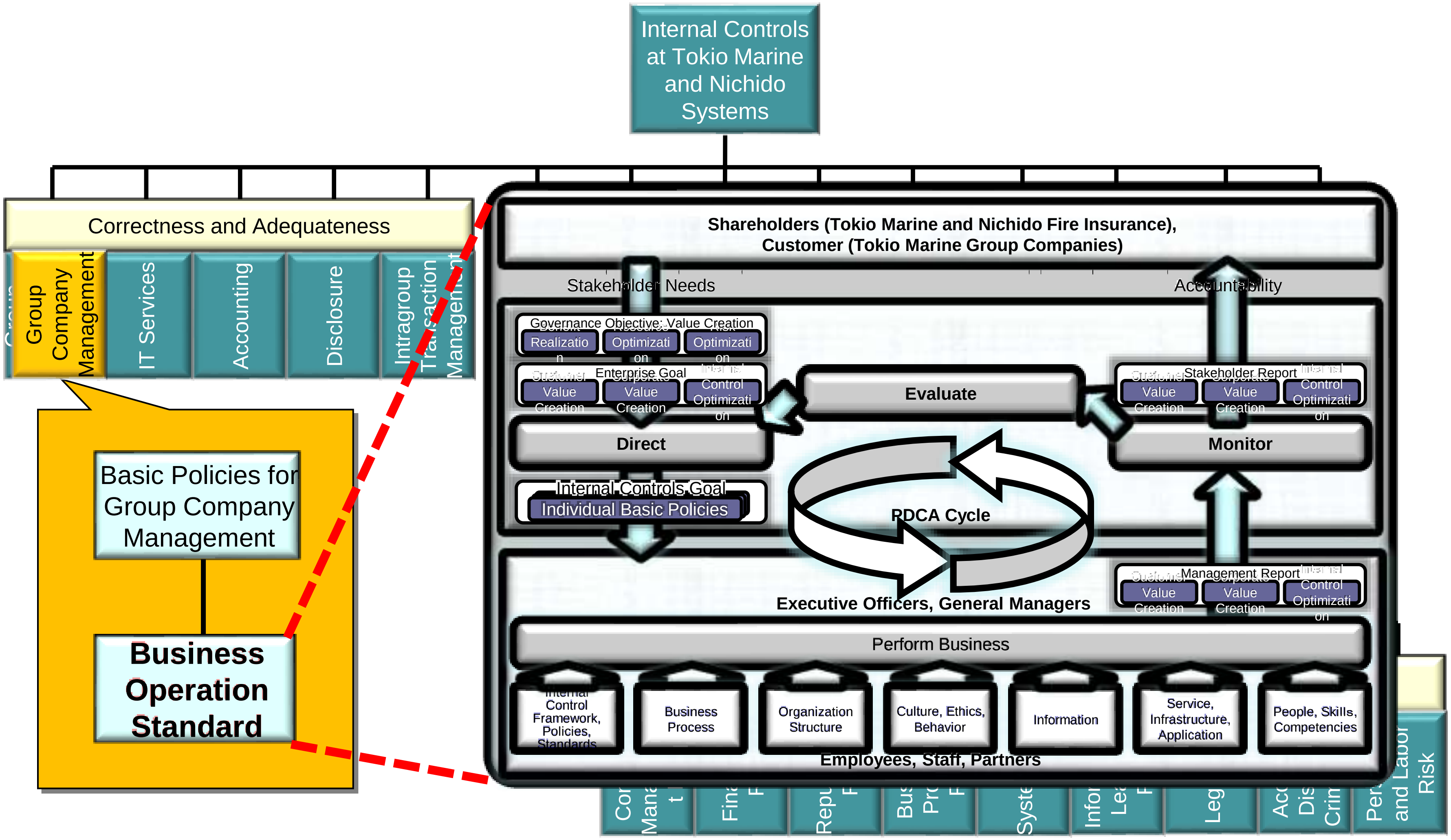
Executive Officers, General Managers

Perform Business

- Internal Control Framework, Policies, Standards
- Business Process
- Organization Structure
- Culture, Ethics, Behavior
- Information
- Service, Infrastructure, Application
- People, Skills, Competencies

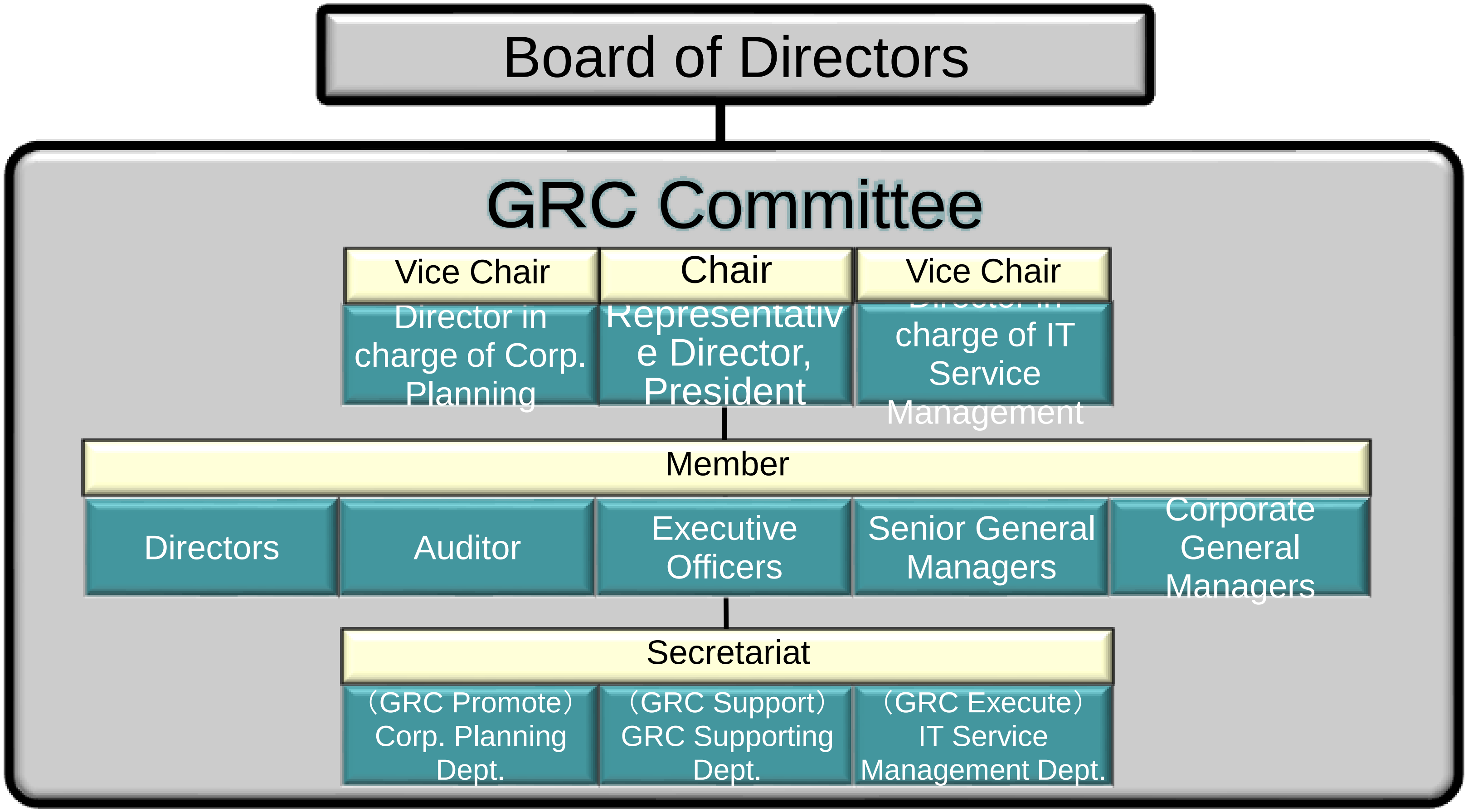
Employees, Staff, Partners

Business Operation Standard was determined by BOD


Internal Controls at Tokio Marine and Nichido Systems
Correctness and Adequateness
Group Company Management
IT Services
Accounting
Disclosure
Intragroup Transaction Management
Basic Policies for Group Company Management
Business Operation Standard
Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)
Stakeholder Needs
Accountability
Governance Objective: Value Creation
Realization
Optimization
Optimization
Enterprise Goal
Value Creation
Value Creation
Control Optimization
Evaluate
Stakeholder Report
Value Creation
Value Creation
Control Optimization
Direct
Monitor
Internal Controls Goal
Individual Basic Policies
PDCA Cycle
Management Report
Value Creation
Value Creation
Control Optimization
Executive Officers, General Managers
Perform Business
Internal Control Framework, Policies, Standards
Business Process
Organization Structure
Culture, Ethics, Behavior
Information
Service, Infrastructure, Application
People, Skills, Competencies
Employees, Staff, Partners
and Labor Risk

Establishment of GRC Committee – Continuous Improvement Engine

- ✓ Existing 3 Committees (Information Security, Compliance, Crisis Management) were integrated into GRC Committee



Board of Directors

GRC Committee

Vice Chair
Director in charge of Corp. Planning

Chair
Representative Director, President

Vice Chair
Director in charge of IT Service Management

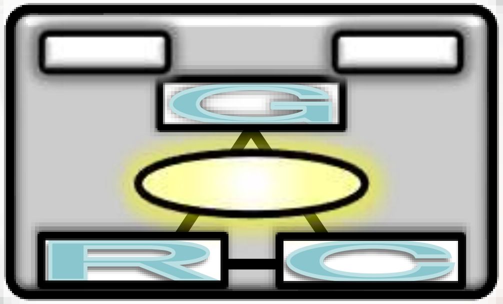
Member
Directors
Auditor
Executive Officers
Senior General Managers
Corporate General Managers

Secretariat
（GRC Promote） Corp. Planning Dept.
（GRC Support） GRC Supporting Dept.
（GRC Execute） IT Service Management Dept.

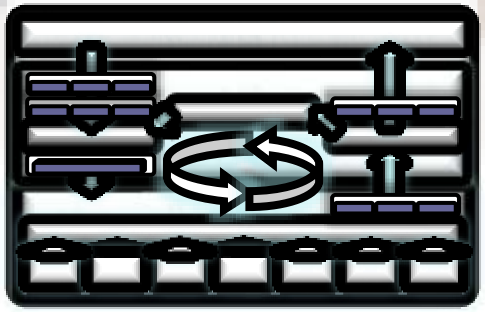
Looking back to the Establishment of GRC System

- ✓ Management has been Steering Company for Value Creation
- ✓ What we achieved is to Visualize it by using the term, “GRC”

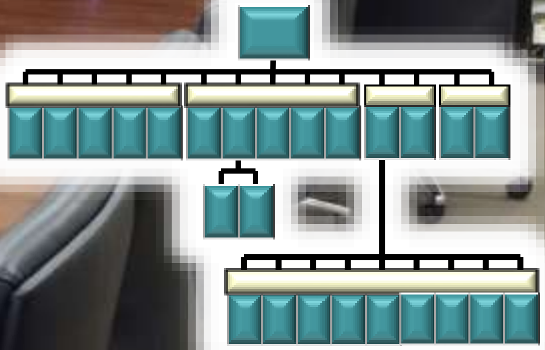
Concept



System



Internal Control



- ✓ Company Management that Ensure Value Creation is Realize
- ✓ How to Manage Company and EDM practices are Important

⇒Enterprise/Management Goals Set-up and their Monitoring

Today’s Contents

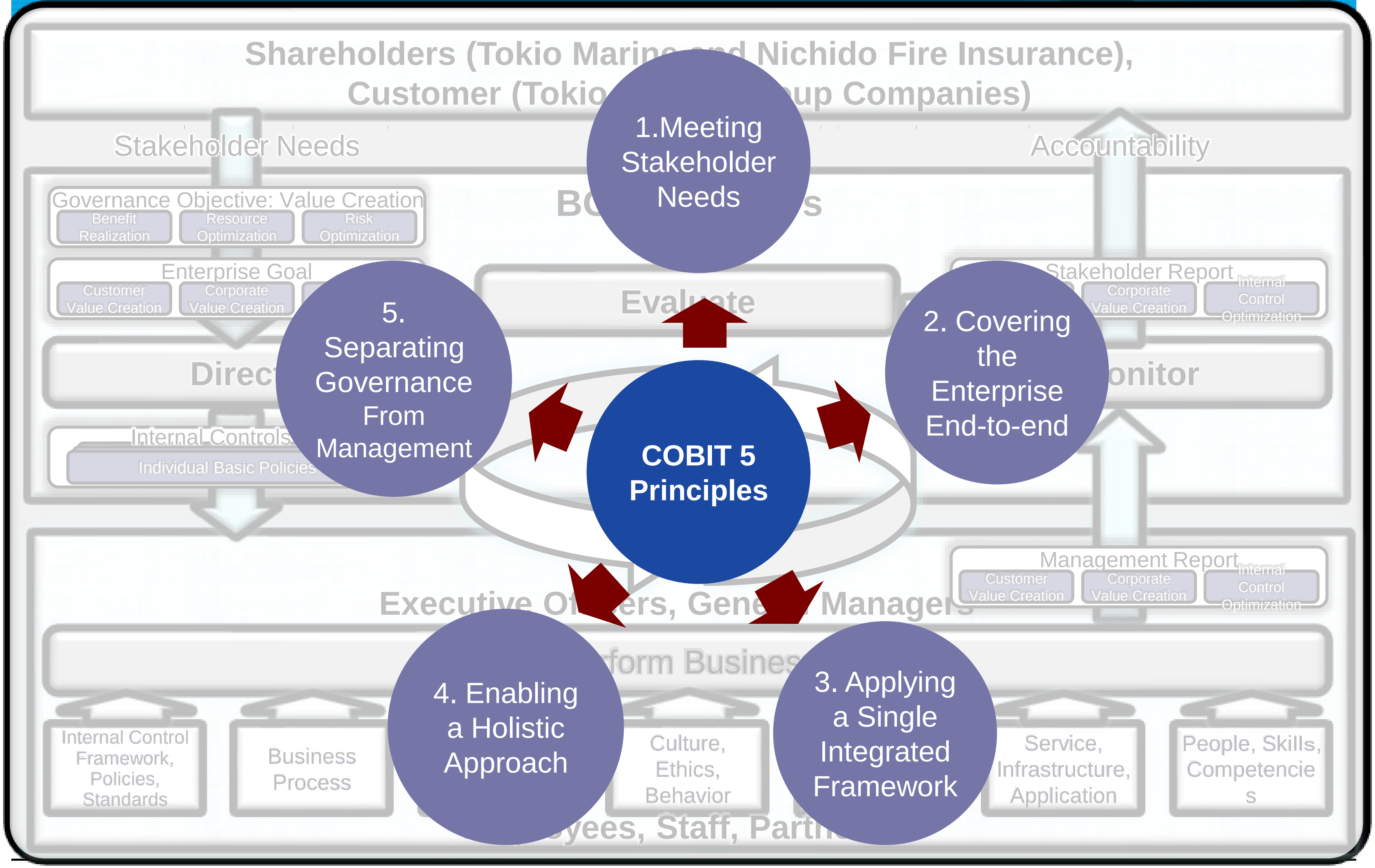
1. Introduction - Myself and My Company

2. From Reactive Internal Control to Proactive GRC

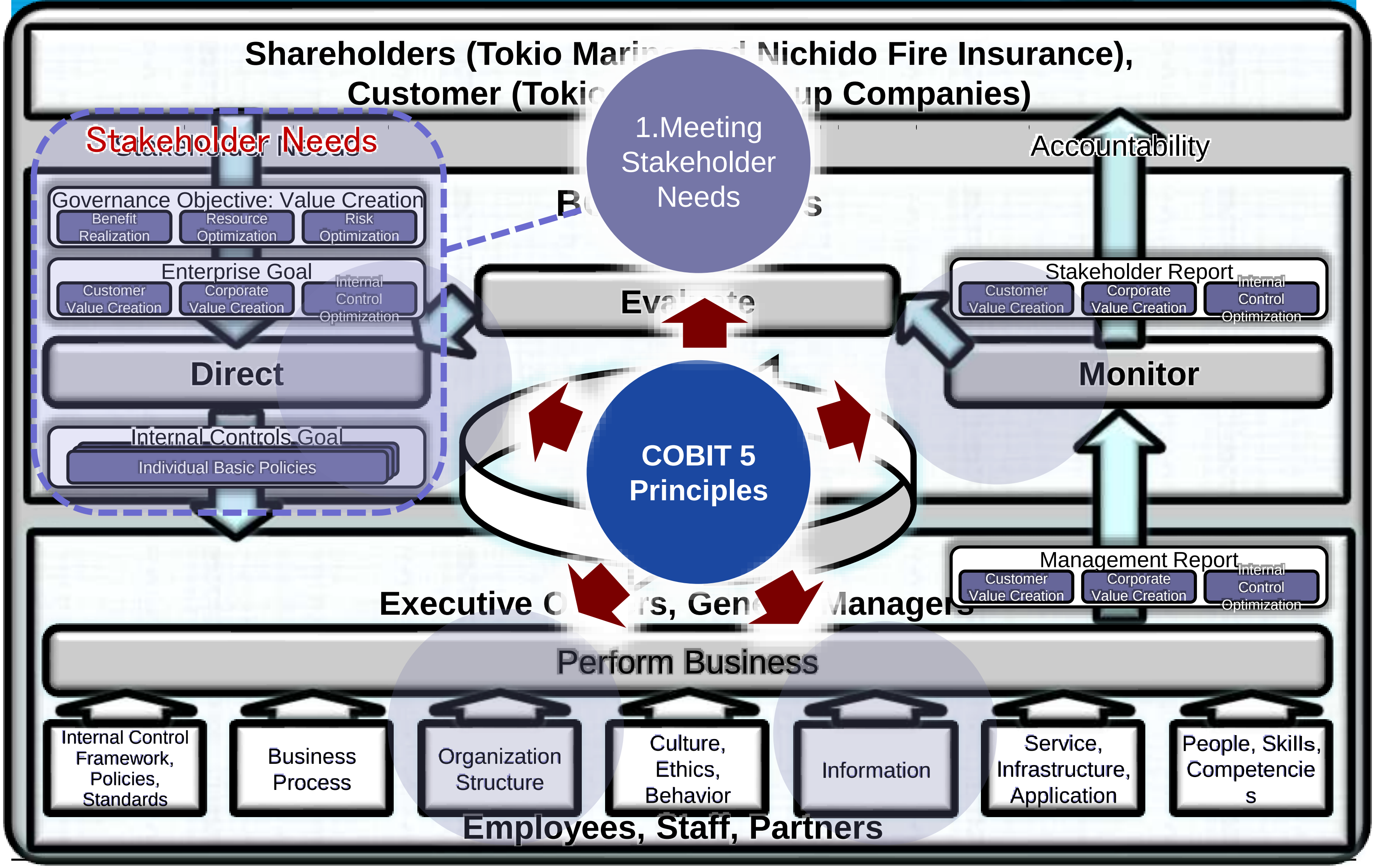
3. GRC at Tokio Marine and Nichido Systems

4. COBIT 5 Empowered and Supported the Change

GRC System based on 5 Principles of COBIT 5


Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio ... up Companies)
Stakeholder Needs
Accountability
Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization
Enterprise Goal
Customer Value Creation
Corporate Value Creation
Stakeholder Report
Corporate Value Creation
Internal Control Optimization
Evaluate
Direct
Monitor
Internal Controls
Individual Basic Policies
Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Executive Officers, General Managers
Perform Business
Internal Control Framework, Policies, Standards
Business Process
Culture, Ethics, Behavior
Service, Infrastructure, Application
People, Skills, Competencies
Employees, Staff, Partners
1.Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

GRC System based on 5 Principles of COBIT 5



Shareholders (Tokio Mari… Nichido Fire Insurance),
Customer (Toki… up Companies)

1.Meeting Stakeholder Needs

Stakeholder Needs

Governance Objective: Value Creation
- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goal
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Direct

Internal Controls Goal
- Individual Basic Policies

B… s

Eva… te

COBIT 5 Principles

Accountability

Stakeholder Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Monitor

Management Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Executive O… rs, Gen… Managers

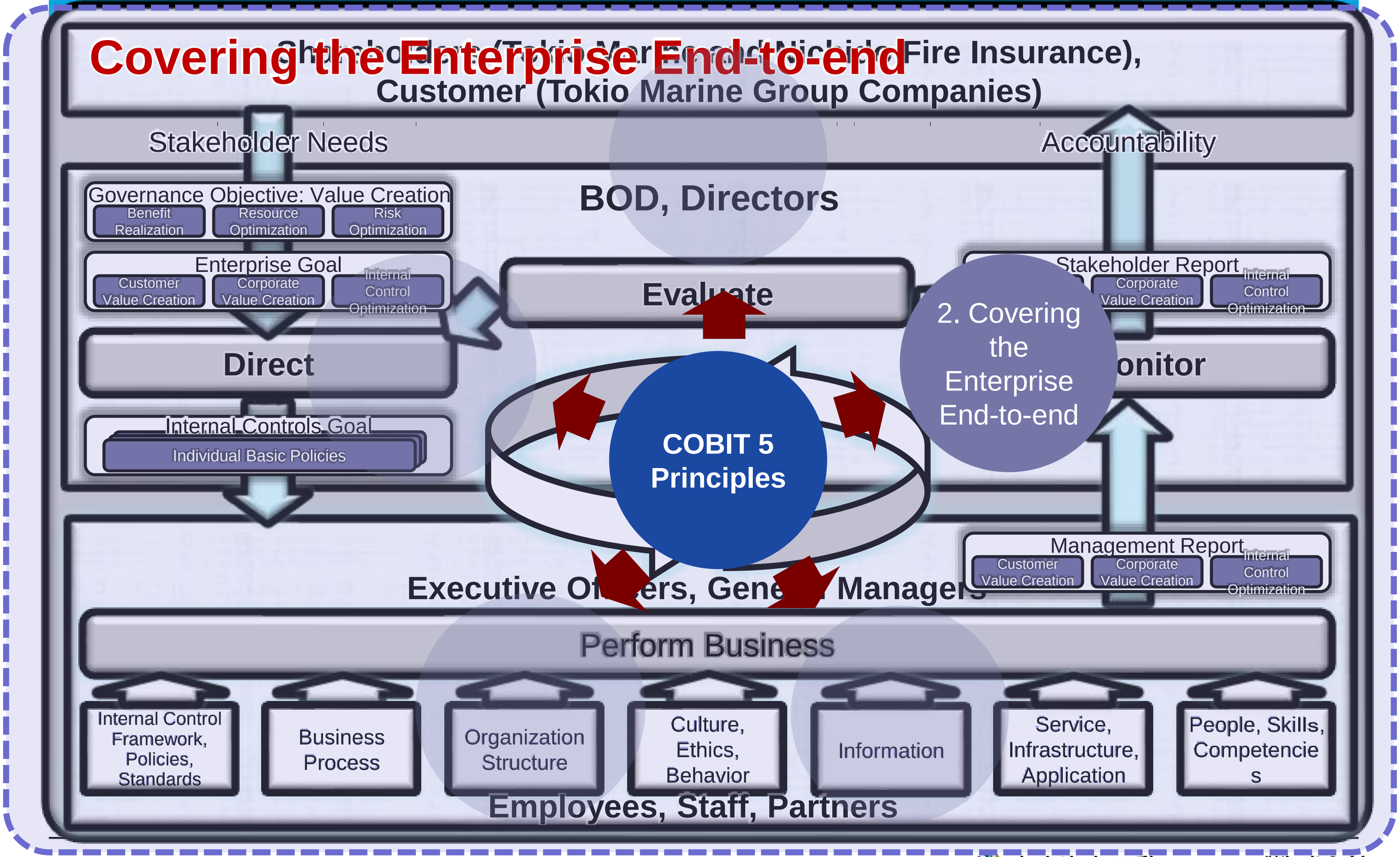
Perform Business

- Internal Control Framework, Policies, Standards
- Business Process
- Organization Structure
- Culture, Ethics, Behavior
- Information
- Service, Infrastructure, Application
- People, Skills, Competencies

Employees, Staff, Partners

GRC System based on 5 Principles of COBIT 5

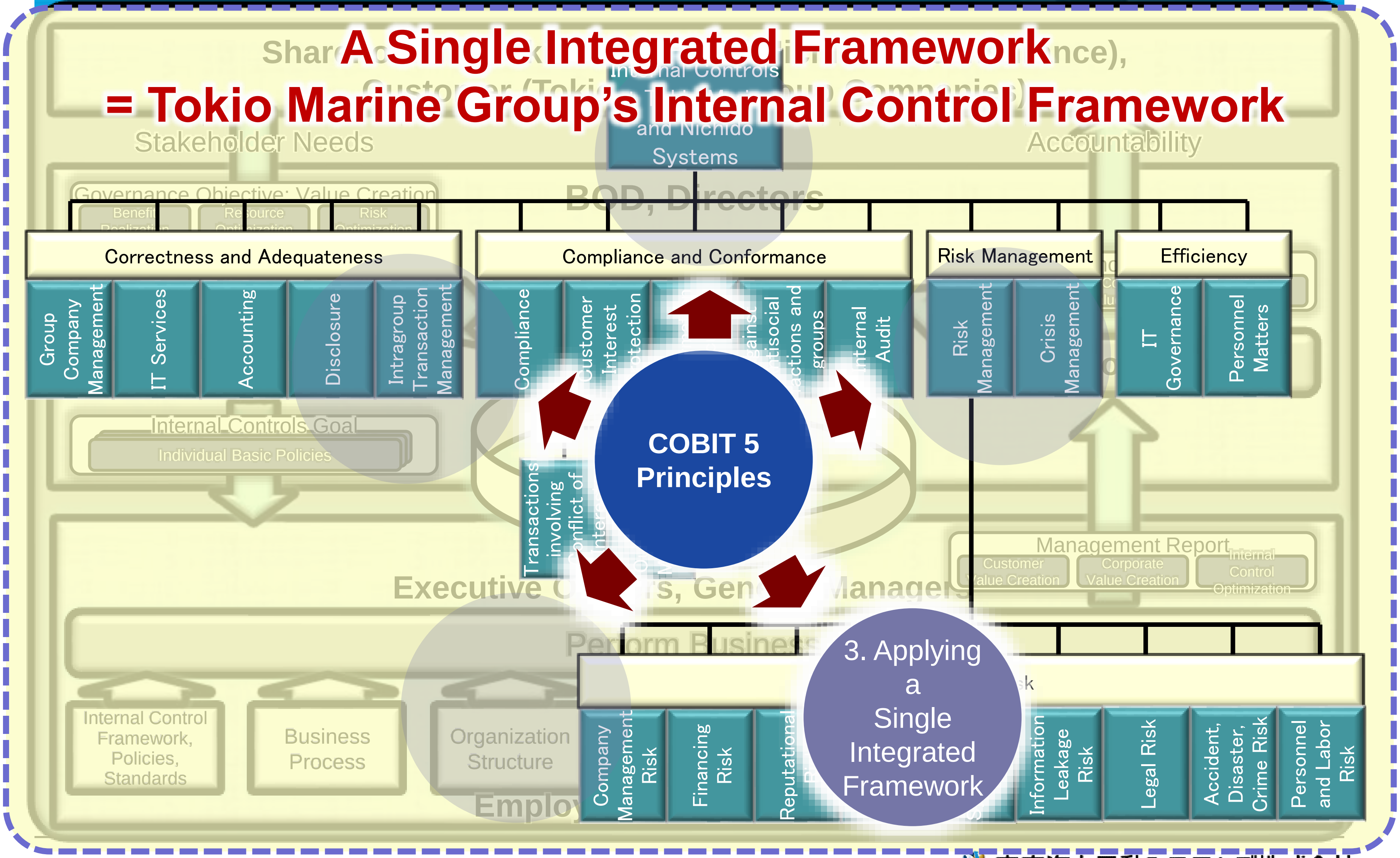
Covering the Enterprise End-to-end


Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)
Stakeholder Needs
Accountability
BOD, Directors
Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization
Enterprise Goal
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Evaluate
Direct
Internal Controls Goal
Individual Basic Policies
Stakeholder Report
Corporate Value Creation
Internal Control Optimization
2. Covering the Enterprise End-to-end
Monitor
COBIT 5 Principles
Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Executive Officers, General Managers
Perform Business
Internal Control Framework, Policies, Standards
Business Process
Organization Structure
Culture, Ethics, Behavior
Information
Service, Infrastructure, Application
People, Skills, Competencies
Employees, Staff, Partners

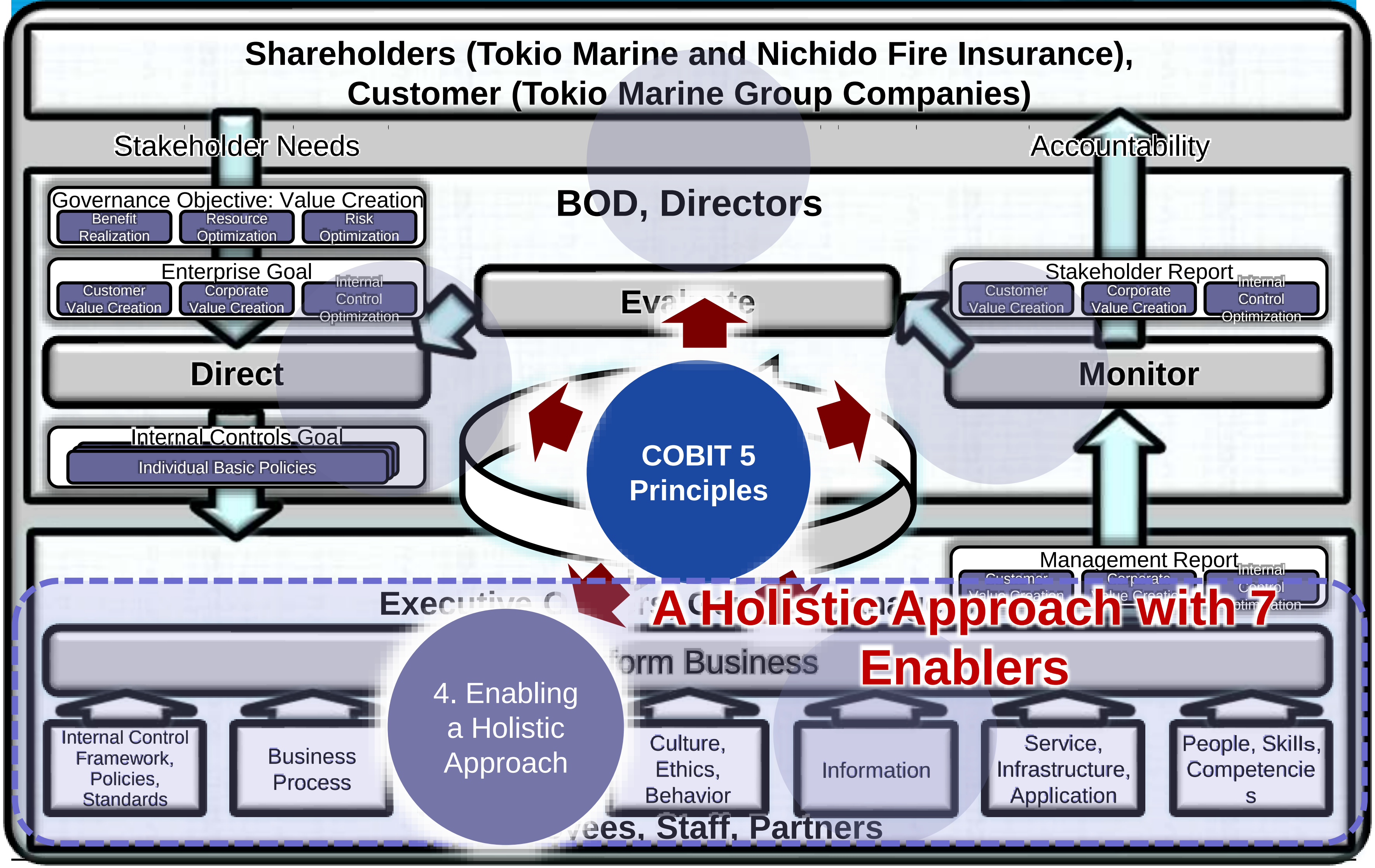
GRC System based on 5 Principles of COBIT 5

A Single Integrated Framework

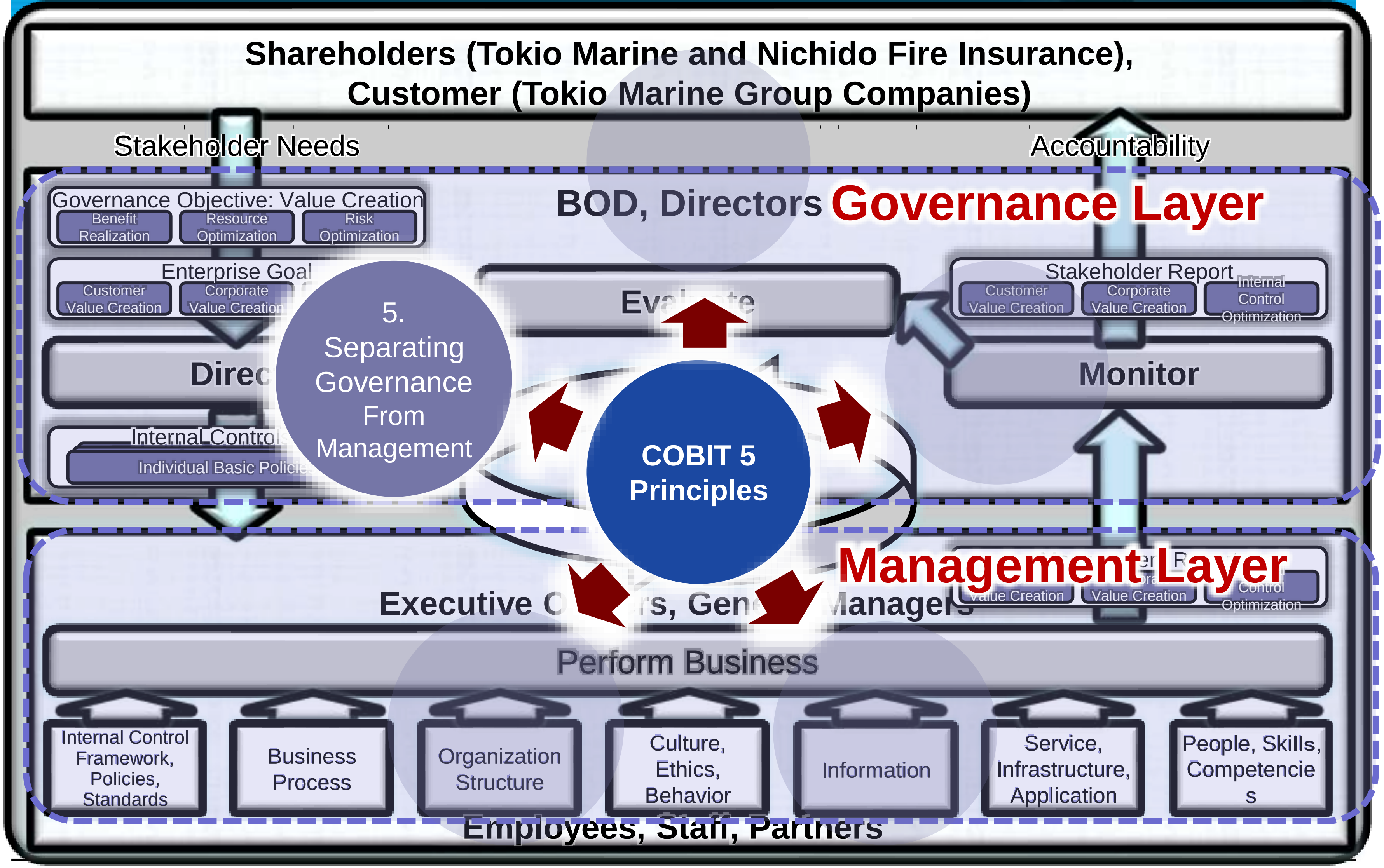
= Tokio Marine Group's Internal Control Framework


Stakeholder Needs
Accountability
Internal Controls
and Nichido
Systems
BOD, Directors
Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization
Correctness and Adequateness
Group Company Management
IT Services
Accounting
Disclosure
Intragroup Transaction Management
Compliance and Conformance
Compliance
Customer Interest Protection
antisocial actions and groups
Internal Audit
Transactions involving conflict of interest
Risk Management
Risk Management
Crisis Management
Efficiency
IT Governance
Personnel Matters
COBIT 5 Principles
Internal Controls Goal
Individual Basic Policies
Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Executive
General Managers
Perform Business
3. Applying a Single Integrated Framework
Company Management Risk
Financing Risk
Reputational Risk
Information Leakage Risk
Legal Risk
Accident, Disaster, Crime Risk
Personnel and Labor Risk
Internal Control Framework, Policies, Standards
Business Process
Organization Structure
Employ

GRC System based on 5 Principles of COBIT 5


Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)
Stakeholder Needs
Accountability
BOD, Directors
Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization
Enterprise Goal
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Eva te
Stakeholder Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Direct
Monitor
Internal Controls Goal
Individual Basic Policies
COBIT 5 Principles
Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Executive C rs
A Holistic Approach with 7 Enablers
orm Business
4. Enabling a Holistic Approach
Internal Control Framework, Policies, Standards
Business Process
Culture, Ethics, Behavior
Information
Service, Infrastructure, Application
People, Skills, Competencies
ees, Staff, Partners

GRC System based on 5 Principles of COBIT 5



Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio Marine Group Companies)

Stakeholder Needs

Accountability

BOD, Directors **Governance Layer**

Governance Objective: Value Creation
- Benefit Realization
- Resource Optimization
- Risk Optimization

Enterprise Goal
- Customer Value Creation
- Corporate Value Creation

Direc

Internal Controls
- Individual Basic Policie

Eva te

Stakeholder Report
- Customer Value Creation
- Corporate Value Creation
- Internal Control Optimization

Monitor

5. Separating Governance From Management

COBIT 5 Principles

Management Layer

er R
- ora
- Value Creation
- Value Creation
- Control Optimization

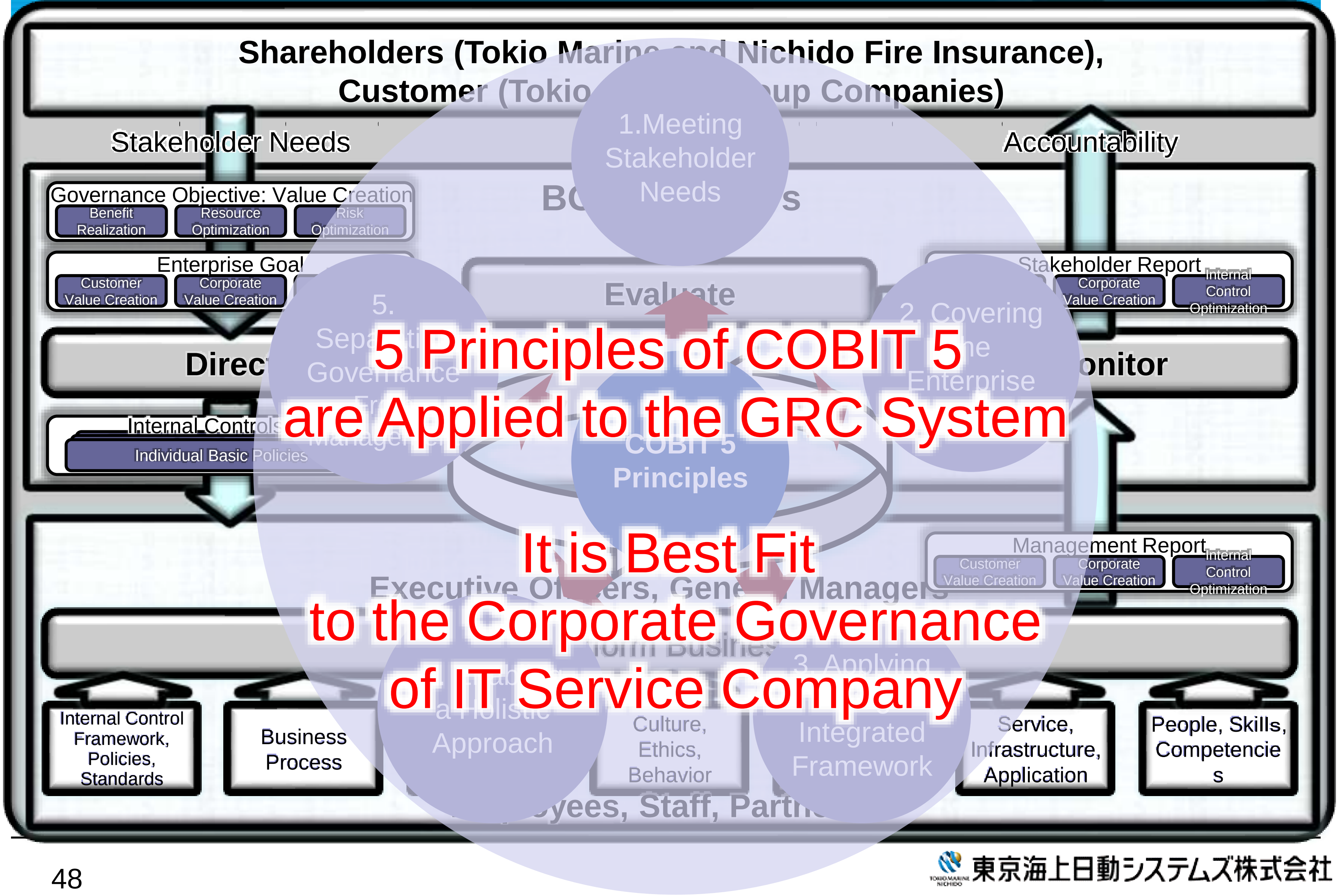
Executive C rs, Gen Managers

Perform Business

- Internal Control Framework, Policies, Standards
- Business Process
- Organization Structure
- Culture, Ethics, Behavior
- Information
- Service, Infrastructure, Application
- People, Skills, Competencies

Employees, Staff, Partners

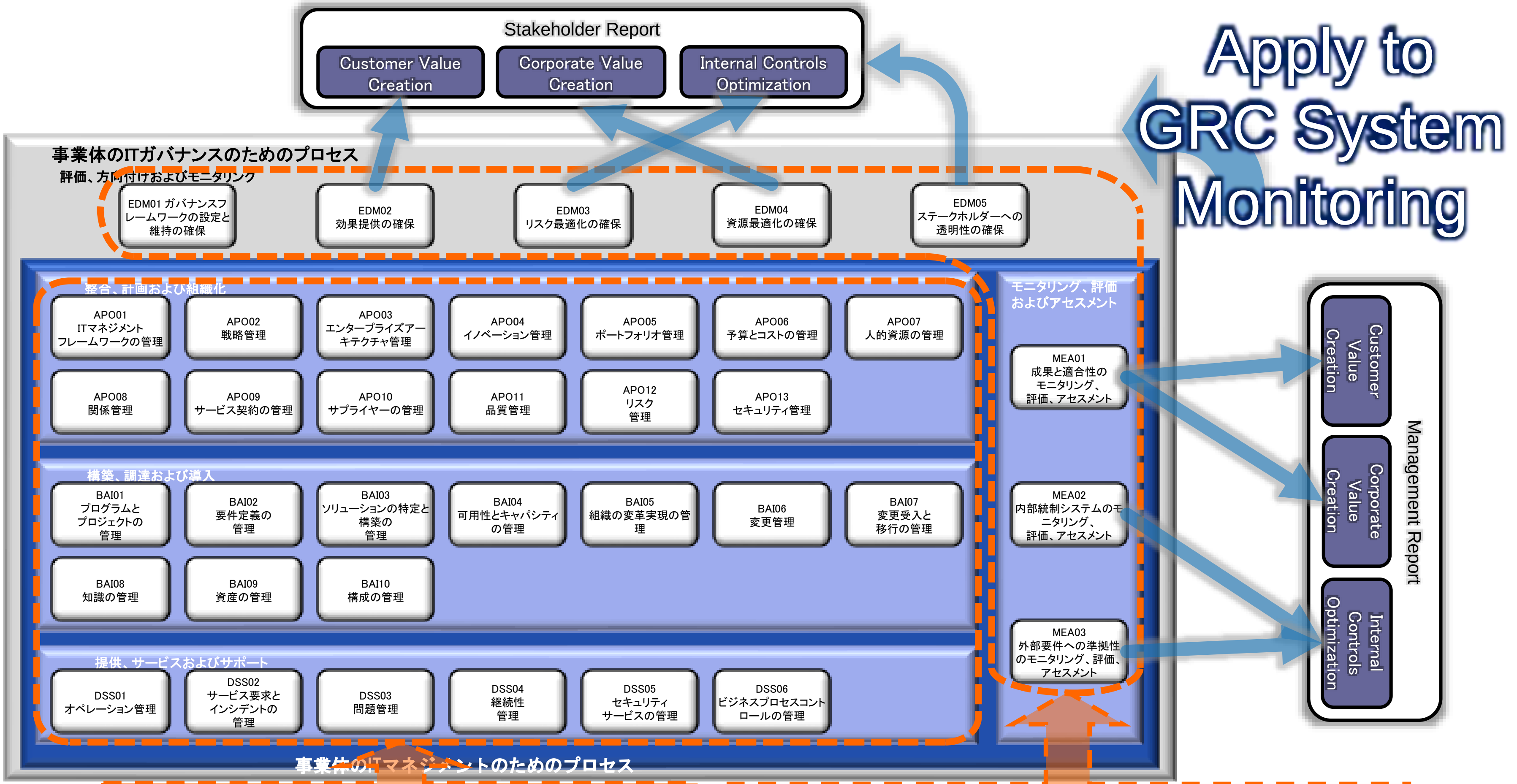
GRC System based on 5 Principles of COBIT 5


Shareholders (Tokio Marine and Nichido Fire Insurance),
Customer (Tokio ... Group Companies)
Stakeholder Needs
Accountability
Governance Objective: Value Creation
Benefit Realization
Resource Optimization
Risk Optimization
Enterprise Goal
Customer Value Creation
Corporate Value Creation
Stakeholder Report
Corporate Value Creation
Internal Control Optimization
Evaluate
Direct
Monitor
Internal Controls
Individual Basic Policies
Management Report
Customer Value Creation
Corporate Value Creation
Internal Control Optimization
Executive Officers, General Managers
Uniform Business
Internal Control Framework, Policies, Standards
Business Process
Culture, Ethics, Behavior
Service, Infrastructure, Application
People, Skills, Competencies
Employees, Staff, Partners
1.Meeting Stakeholder Needs
2. Covering the Enterprise
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

5 Principles of COBIT 5 are Applied to the GRC System

It is Best Fit to the Corporate Governance of IT Service Company

Utilize COBIT 5 Process Reference Model



Stakeholder Report

Customer Value Creation

Corporate Value Creation

Internal Controls Optimization

Apply to GRC System Monitoring

事業体のITガバナンスのためのプロセス

評価、方向付けおよびモニタリング

- EDM01 ガバナンスフレームワークの設定と維持の確保
- EDM02 効果提供の確保
- EDM03 リスク最適化の確保
- EDM04 資源最適化の確保
- EDM05 ステークホルダーへの透明性の確保

整合、計画および組織化

- APO01 ITマネジメントフレームワークの管理
- APO02 戦略管理
- APO03 エンタープライズアーキテクチャ管理
- APO04 イノベーション管理
- APO05 ポートフォリオ管理
- APO06 予算とコストの管理
- APO07 人的資源の管理
- APO08 関係管理
- APO09 サービス契約の管理
- APO10 サプライヤーの管理
- APO11 品質管理
- APO12 リスク管理
- APO13 セキュリティ管理

構築、調達および導入

- BAI01 プログラムとプロジェクトの管理
- BAI02 要件定義の管理
- BAI03 ソリューションの特定と構築の管理
- BAI04 可用性とキャパシティの管理
- BAI05 組織の変革実現の管理
- BAI06 変更管理
- BAI07 変更受入と移行の管理
- BAI08 知識の管理
- BAI09 資産の管理
- BAI10 構成の管理

提供、サービスおよびサポート

- DSS01 オペレーション管理
- DSS02 サービス要求とインシデントの管理
- DSS03 問題管理
- DSS04 継続性管理
- DSS05 セキュリティサービスの管理
- DSS06 ビジネスプロセスコントロールの管理

モニタリング、評価およびアセスメント

- MEA01 成果と適合性のモニタリング、評価、アセスメント
- MEA02 内部統制システムのモニタリング、評価、アセスメント
- MEA03 外部要件への準拠性のモニタリング、評価、アセスメント

事業体のITマネジメントのためのプロセス

Management Report

Customer Value Creation

Corporate Value Creation

Internal Controls Optimization

Specific to IT Domain

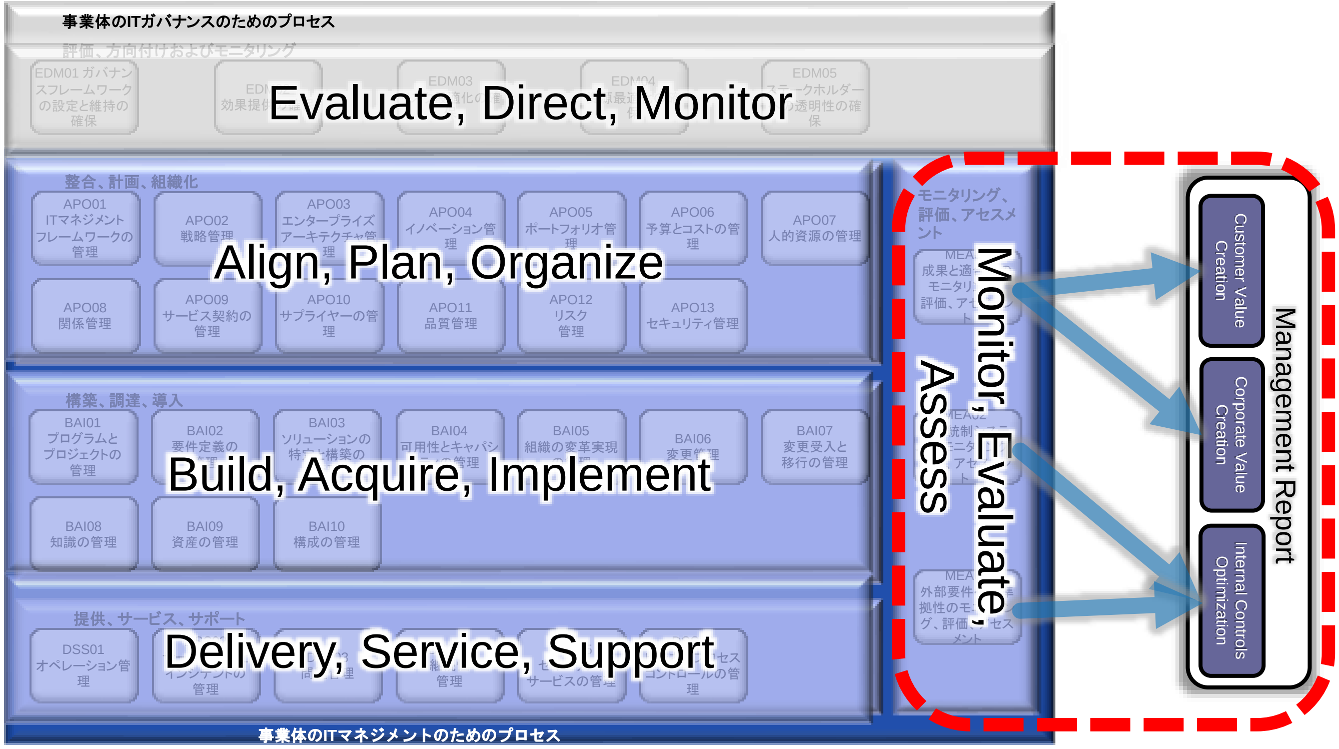
➡ Apply to IT related Domains

Applicable to all Domains

➡ Apply to overall GRC (Monitoring)

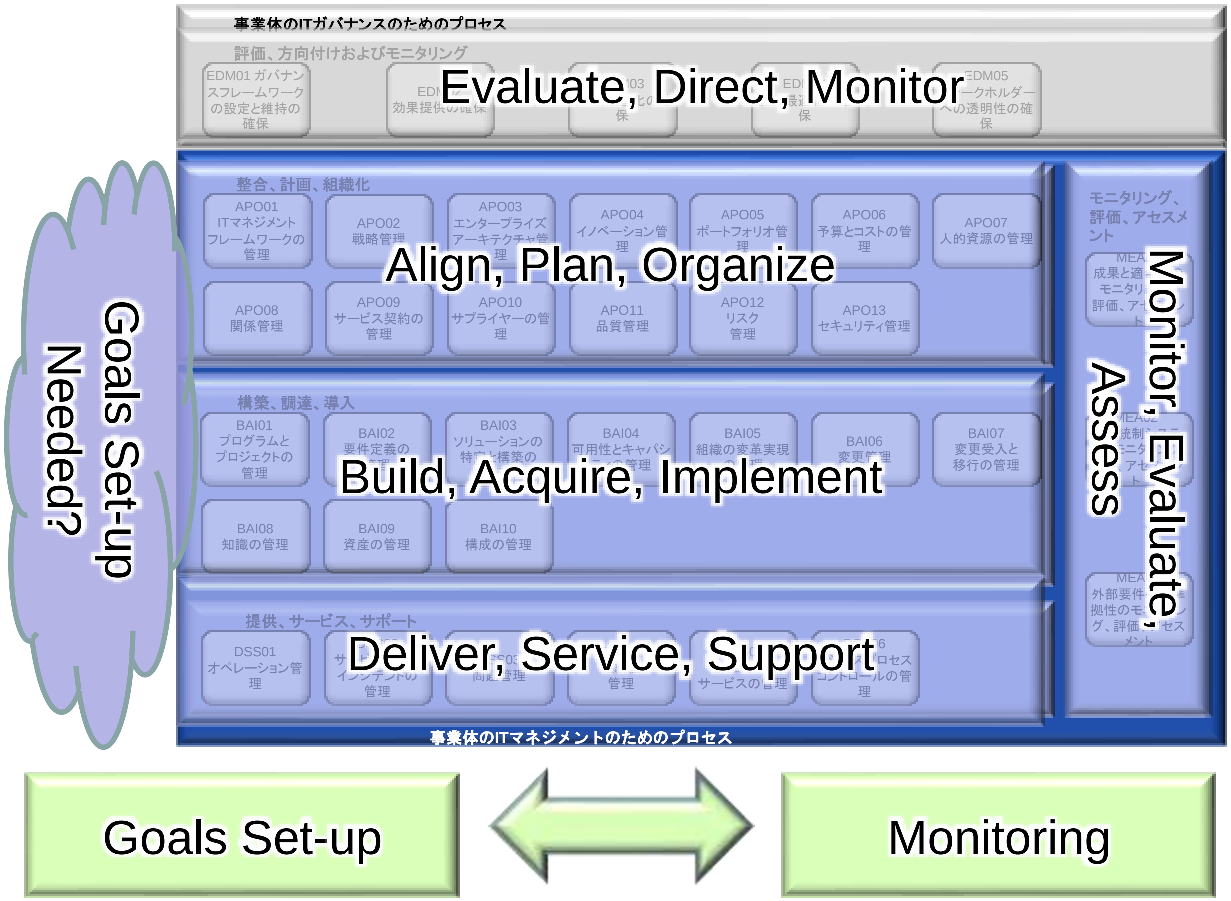
Analyze COBIT 5 Process Reference Model

✓ Monitoring (MEA Domain) is Applied to overall GRC


事業体のITガバナンスのためのプロセス
評価、方向付けおよびモニタリング
EDM01 ガバナンスフレームワークの設定と維持の確保
EDM05 ステークホルダーの透明性の確保
Evaluate, Direct, Monitor
整合、計画、組織化
APO01 ITマネジメントフレームワークの管理
APO02 戦略管理
APO03 エンタープライズアーキテクチャ管理
APO04 イノベーション管理
APO05 ポートフォリオ管理
APO06 予算とコストの管理
APO07 人的資源の管理
APO08 関係管理
APO09 サービス契約の管理
APO10 サプライヤーの管理
APO11 品質管理
APO12 リスク管理
APO13 セキュリティ管理
Align, Plan, Organize
構築、調達、導入
BAI01 プログラムとプロジェクトの管理
BAI02 要件定義の管理
BAI03 ソリューションの特定と構築の管理
BAI04 可用性とキャパシティの管理
BAI05 組織の変革実現の管理
BAI06 変更管理
BAI07 変更受入と移行の管理
BAI08 知識の管理
BAI09 資産の管理
BAI10 構成の管理
Build, Acquire, Implement
提供、サービス、サポート
DSS01 オペレーション管理
Delivery, Service, Support
事業体のITマネジメントのためのプロセス
モニタリング、評価、アセスメント
Monitor, Evaluate, Assess
Management Report
Customer Value Creation
Corporate Value Creation
Internal Controls Optimization

Analyze COBIT 5 Process Reference Model

- ✓ There should be Goals Set-up for Monitoring



Evaluate, Direct, Monitor

Align, Plan, Organize

Build, Acquire, Implement

Deliver, Service, Support

Monitor, Evaluate, Assess

Goals Set-up Needed?

Goals Set-up

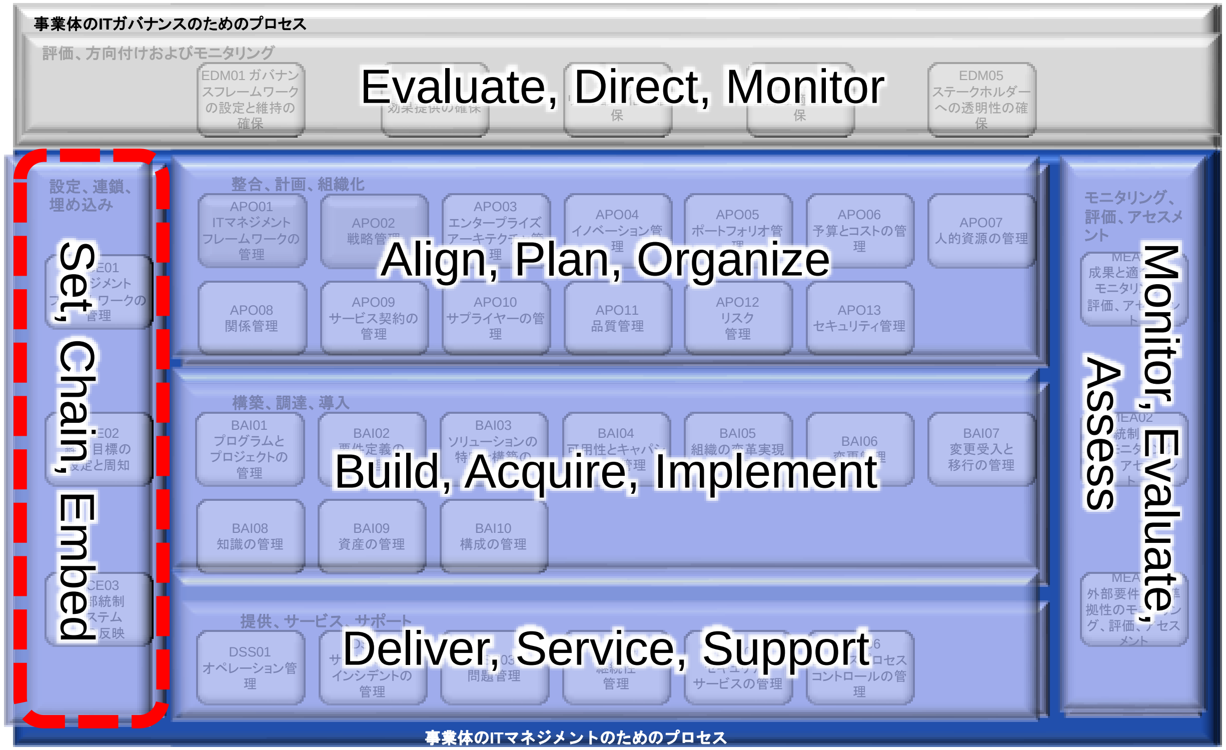
Monitoring

事業体のITガバナンスのためのプロセス
評価、方向付けおよびモニタリング
EDM01 ガバナンスフレームワークの設定と維持の確保
EDM02 効果提供の確保
EDM03
EDM04
EDM05 ステークホルダーへの透明性の確保
整合、計画、組織化
APO01 ITマネジメントフレームワークの管理
APO02 戦略管理
APO03 エンタープライズアーキテクチャ管理
APO04 イノベーション管理
APO05 ポートフォリオ管理
APO06 予算とコストの管理
APO07 人的資源の管理
APO08 関係管理
APO09 サービス契約の管理
APO10 サプライヤーの管理
APO11 品質管理
APO12 リスク管理
APO13 セキュリティ管理
構築、調達、導入
BAI01 プログラムとプロジェクトの管理
BAI02 要件定義の管理
BAI03 ソリューションの特定と構築の管理
BAI04 可用性とキャパシティの管理
BAI05 組織の変革実現の管理
BAI06 変更管理
BAI07 変更受入と移行の管理
BAI08 知識の管理
BAI09 資産の管理
BAI10 構成の管理
提供、サービス、サポート
DSS01 オペレーション管理
DSS02 サービス要求とインシデントの管理
DSS03 問題管理
DSS04 継続性管理
DSS05 セキュリティサービスの管理
DSS06 ビジネスプロセスコントロールの管理
モニタリング、評価、アセスメント
MEA01 成果と適合性のモニタリング、評価、アセスメント
MEA02 内部統制システムのモニタリング、評価、アセスメント
MEA03 外部要件への準拠性のモニタリング、評価、アセスメント
事業体のITマネジメントのためのプロセス

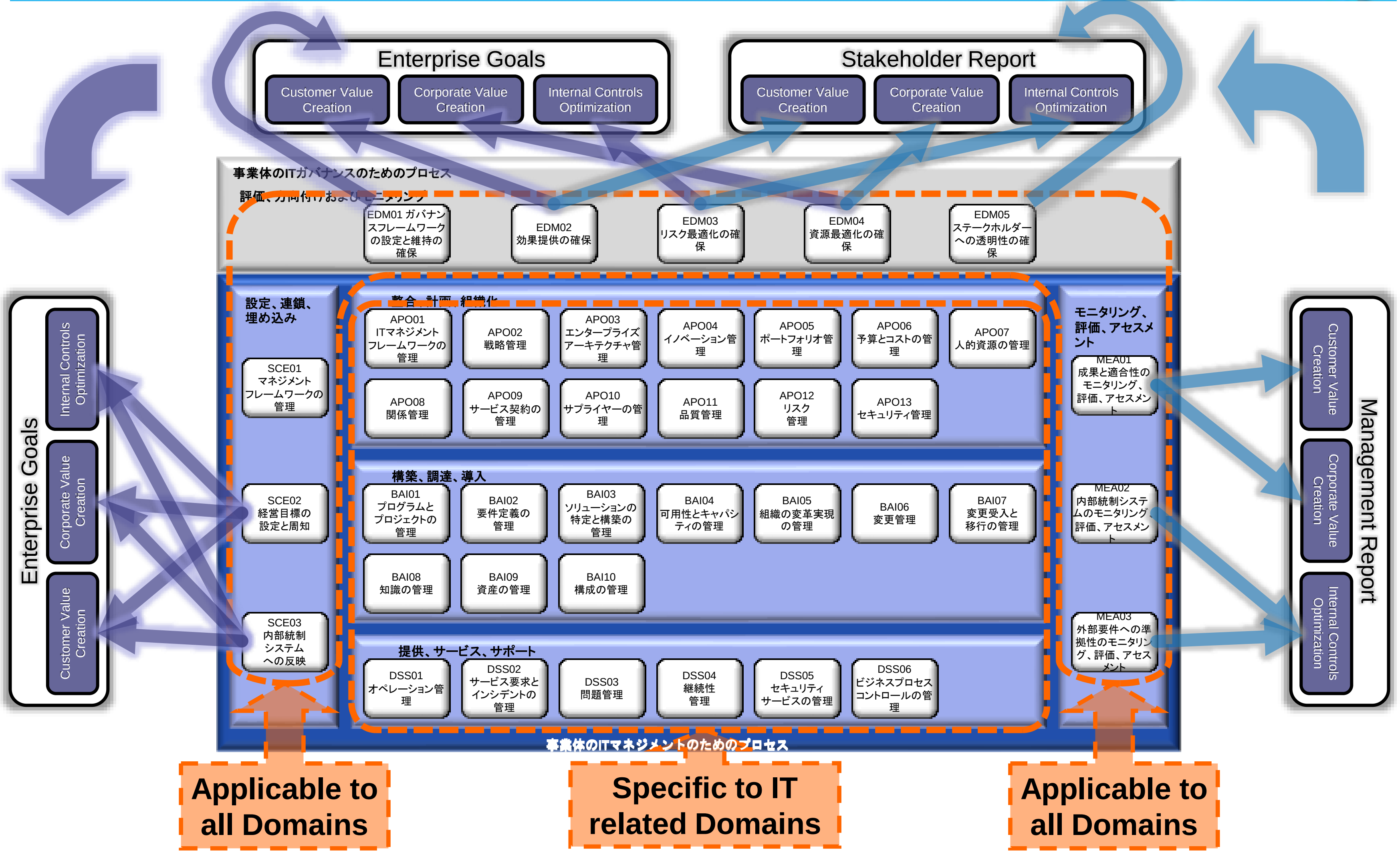
Tentatively Define “Set, Chain, Embed” Domain

✓Tentatively Define Goals Set-up Processes for Overall GRC

1.Set-up Management Goals, 2.Chain to BU Goals, 3.Embed into Internal Control

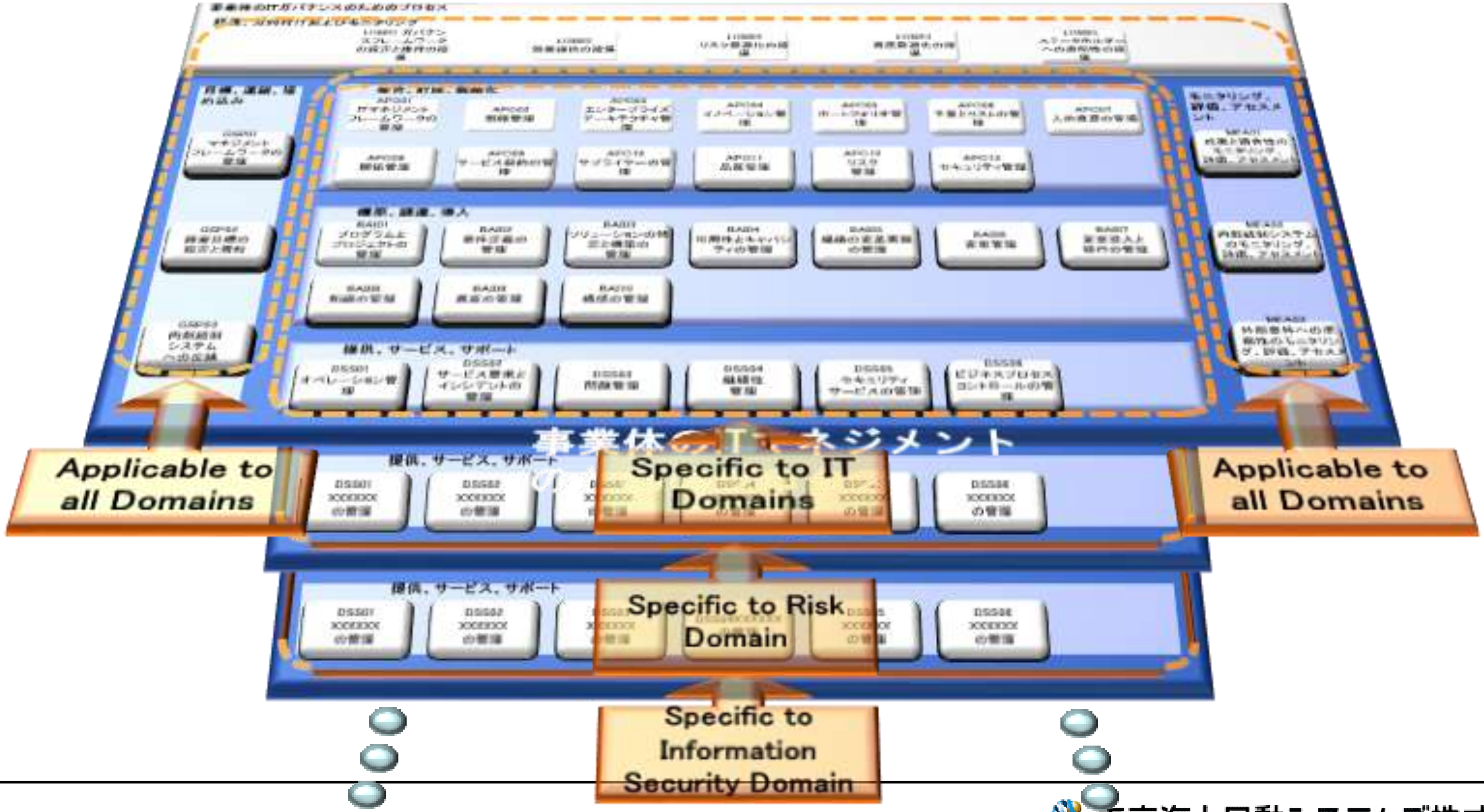

事業体のITガバナンスのためのプロセス
評価、方向付けおよびモニタリング
EDM01 ガバナンスフレームワークの設定と維持の確保
EDM05 ステークホルダーへの透明性の確保
Evaluate, Direct, Monitor
設定、連鎖、埋め込み
Set, Chain, Embed
整合、計画、組織化
APO01 ITマネジメントフレームワークの管理
APO02 戦略管理
APO03 エンタープライズアーキテクチャ管理
APO04 イノベーション管理
APO05 ポートフォリオ管理
APO06 予算とコストの管理
APO07 人的資源の管理
APO08 関係管理
APO09 サービス契約の管理
APO10 サプライヤーの管理
APO11 品質管理
APO12 リスク管理
APO13 セキュリティ管理
Align, Plan, Organize
構築、調達、導入
BAI01 プログラムとプロジェクトの管理
BAI02
BAI03 ソリューションの
BAI04
BAI05 組織の変革実現
BAI06
BAI07 変更受入と移行の管理
BAI08 知識の管理
BAI09 資産の管理
BAI10 構成の管理
Build, Acquire, Implement
提供、サービス、サポート
DSS01 オペレーション管理
インシデントの管理
問題管理
管理
サービスの管理
コントロールの管理
Deliver, Service, Support
モニタリング、評価、アセスメント
Monitor, Evaluate, Assess
事業体のITマネジメントのためのプロセス

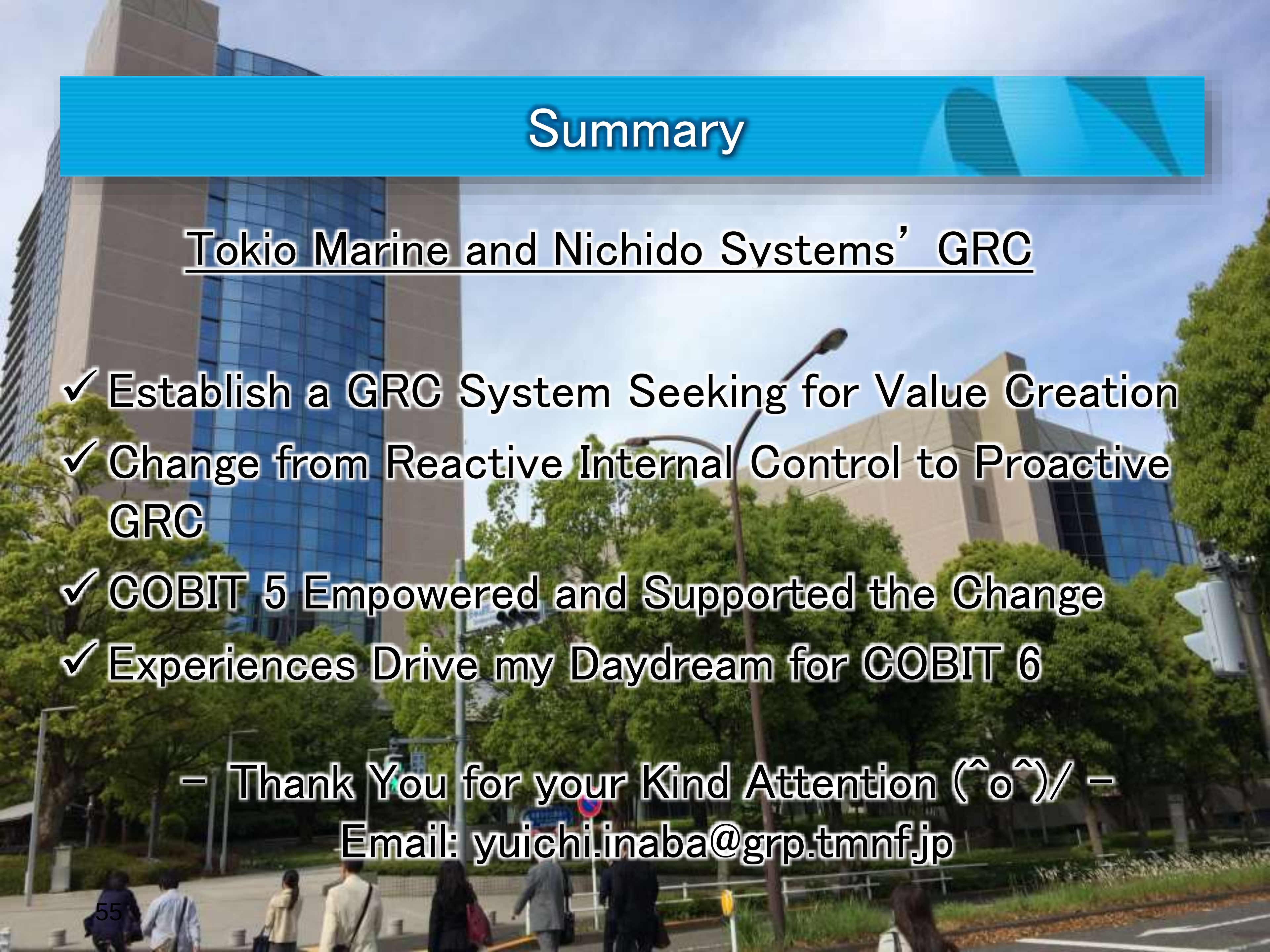
PRM which Fits to Our GRC System


Enterprise Goals
Customer Value Creation
Corporate Value Creation
Internal Controls Optimization
Stakeholder Report
Customer Value Creation
Corporate Value Creation
Internal Controls Optimization
事業体のITガバナンスのためのプロセス
評価、方向付けおよびモニタリング
EDM01 ガバナンスフレームワークの設定と維持の確保
EDM02 効果提供の確保
EDM03 リスク最適化の確保
EDM04 資源最適化の確保
EDM05 ステークホルダーへの透明性の確保
設定、連鎖、埋め込み
SCE01 マネジメントフレームワークの管理
SCE02 経営目標の設定と周知
SCE03 内部統制システムへの反映
整合、計画、組織化
APO01 ITマネジメントフレームワークの管理
APO02 戦略管理
APO03 エンタープライズアーキテクチャ管理
APO04 イノベーション管理
APO05 ポートフォリオ管理
APO06 予算とコストの管理
APO07 人的資源の管理
APO08 関係管理
APO09 サービス契約の管理
APO10 サプライヤーの管理
APO11 品質管理
APO12 リスク管理
APO13 セキュリティ管理
構築、調達、導入
BAI01 プログラムとプロジェクトの管理
BAI02 要件定義の管理
BAI03 ソリューションの特定と構築の管理
BAI04 可用性とキャパシティの管理
BAI05 組織の変革実現の管理
BAI06 変更管理
BAI07 変更受入と移行の管理
BAI08 知識の管理
BAI09 資産の管理
BAI10 構成の管理
提供、サービス、サポート
DSS01 オペレーション管理
DSS02 サービス要求とインシデントの管理
DSS03 問題管理
DSS04 継続性管理
DSS05 セキュリティサービスの管理
DSS06 ビジネスプロセスコントロールの管理
モニタリング、評価、アセスメント
MEA01 成果と適合性のモニタリング、評価、アセスメント
MEA02 内部統制システムのモニタリング、評価、アセスメント
MEA03 外部要件への準拠性のモニタリング、評価、アセスメント
事業体のITマネジメントのためのプロセス
Enterprise Goals
Internal Controls Optimization
Corporate Value Creation
Customer Value Creation
Management Report
Customer Value Creation
Corporate Value Creation
Internal Controls Optimization
Applicable to all Domains
Specific to IT related Domains
Applicable to all Domains

Might be one example of COBIT 6 …

- ✓ EDM, SCE, MEA are Common Domains
- ✓ APO, BAI, DSS are Specific to Each Domain
- ✓ Move from GEIT to Corporate Governance


事業体のITマネジメント
Applicable to all Domains
Specific to IT Domains
Applicable to all Domains
Specific to Risk Domain
Specific to Information Security Domain



Summary

Tokio Marine and Nichido Systems' GRC

- ✓ Establish a GRC System Seeking for Value Creation
- ✓ Change from Reactive Internal Control to Proactive GRC
- ✓ COBIT 5 Empowered and Supported the Change
- ✓ Experiences Drive my Daydream for COBIT 6

– Thank You for your Kind Attention (^o^)/ –
Email: yuichi.inaba@grp.tmnf.jp