

Bab VI : IT Policy Compliance



Dr. Ir. Yeffry Handoko Putra, M.T

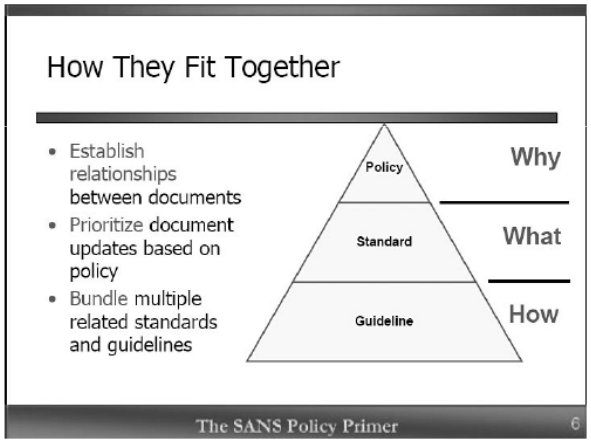
Policy

- **Policy protects people and information. Without policy the organization is like a ship without a rudder. Most critically, policy is the primary guideline against which an audit is conducted. If the policy and procedures are lacking, the audit will also lack rigor.**
- **SMART methodology consists of the following components:**
  - **S**pecific Detail each component
  - **M**easurable Ensure that your record sizes, times and other relevant material
  - **A**chievable Ensure that you have the resources to achieve your objectives
  - **R**ealistic Report the facts; don't speculate
  - **T**ime-based Both work to time constraints and deadlines and ensure that you recorded all the events as they have occurred on the system.

IT Policy

- **Compliance**
- **Security**
- **Standards and Frameworks : CIS, CobIT**
- **regulations**
- **related professional associations**

Policy Standard and Guidelines



Compliance (Kepatuhan)?

- Compliance berarti kepatuhan (Conformity) atau bertindah sesuai standar yang ditetapkan
- Compliance bisa berupa peraturan-peraturan yang membuat suatu perusahaan dapat beroperasi
- Secara praktris compliance diartikan dengan kepatuhan terhadap hukum
- assisting IT management and auditing professionals in meeting compliance requirements.

IT Policy Compliance

- *IT policy compliance is the implementation and management of* information technology in accordance with accepted standards.
- The applicability of standards to your organization dependson a variety of factors, including:
  - The nature of your business.
  - The types of data being processed by your organization.
  - The risks that apply to your environment.

Standard and Framework

source: http://www.itpolicycompliance.com/resources/standards_and_frameworks_links/

- CIS (Center for Internet Security)
- CobIT
- CVE (Common Vulnerabilities and Exposures)
- Guide to Assessment of IT General Controls Scope based on Risk (GAIT)
- Global Technology Audit Guide (GTAG)
- HIPAA
- ISO 27000 and ISO 27001
- ISO 38500 for IT Corporate Governance
- ITIL
- NERC
- NIST

Benefit of apply IT Policy Compliance

- Monitor a larger range of transactions, controls, and systems than a person could ever assess using a manual process.
- Provide a level of consistency that eliminates the subjectivity of human review.
- Run metrics and reports that ultimately help you manage the quality of both your compliance program and operations overall.

Ecosystem in IT Policy Compliance

- Organizational strategic objectives.
- User awareness and training.
- High-level policies.
- Procedures and standards.
- Configuration settings.
- Technology controls.
- Ongoing monitoring.
- Business risk assessments.
- Internal and external auditors.

Regulations vs. Standards vs. Auditors



example sources of government and industry standards that affect IT policy compliance

- Control Objectives for Information and Related IT (COBIT).
- National Institute of Standards and Technology (NIST) standards.
- International Standards Organization (ISO) 27001.
- Information Technology Infrastructure Library (ITIL).
- Payment Card Industry Data Security Standard (PCI DSS).
- NERC Critical Infrastructure Protection (CIP) standards.
- Federal Financial Institution Examination Council (FFIEC) Information Security Book.
- Security Content Automation Protocol (SCAP).

Examples of government- and industry-certified auditors responsible for verifying IT policy compliance

- Internal auditors employed by an organization.
- Certified Public Accountants (CPAs).
- Bank auditors, such as those from the Federal Reserve,
- Federal Depository Trust Corporation (FDIC), and Officeof Comptroller of the Currency (OCC).
- Payment Card Industry (PCI) Qualified Security Assessors (QSAs)./

Making Sense of It All

- What law(s) apply to my company or agency?
- What standards help to guide us toward compliance with those laws?
- What type of audits and assessments are required for compliance?
- What controls do we need in place to meet policyrequirements?
- What evidence do we need to substantiate compliance to auditors?

examples of areas of responsibility and the related laws that affect IT policy compliance (US)

- Financial reporting and accountability: Sarbanes–Oxley Act of 2002.
- Non-public personal information, including financial information: Gramm – Leach-Bliley Act of 1999 (GBLA).
- Protected health information: Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Energy regulation and authority of federal agencies such as U.S. Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC): Energy Policy Act of 2005.
- Personal information breach notification: California SB 1386 and the American Recovery and Reinvestment Act of 2009 (ARRA).
- Government computer security: Federal Information Security Management Act of 2002 (FISMA).
- Personal data: UK Data Protection Act of 1995.

Step by step making and implementing IT Policy

1. Determine the policy problem : content and environ. aspect
2. Using standar
3. Sensitivity of policy
4. Ecosystem of policy
5. Implementing strategy

Contoh 1:
Contoh 2

Audit Risk

- Audit risk = Inherent risk × Control risk × Detection risk
- *Inherent risk means things that are built into the audit* situation and that the auditor doesn't control, such as type of business, type of activity, or other environmental factors.
- *Control risk refers to the likelihood that the control* environment won't detect or prevent an error or misstatement. When the client designs a better control environment, it automatically reduces control and audit risks.
- *Detection risk is the likelihood that an error or misstatement* won't be captured by an auditor's testing. This area of audit risk is the one over which an auditor has the most control.

Align IT Policy Compliance and Security with the Business

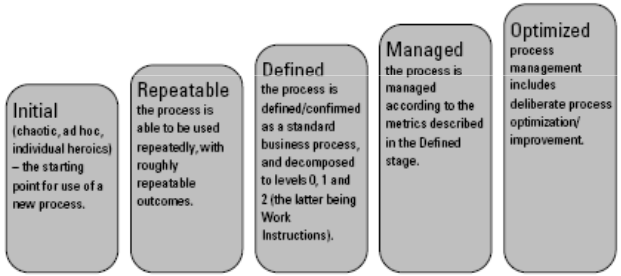


Figure 3-1: The SEI Common Maturity Model.

Indonesia 12 Key Standard for financial system

12 Key Standards for Sound Financial Systems	Compliance Level
Special Data Dissemination Standard	CP
Code of Good Practices on Transparency in Monetary Policy	CP
Code of Good Practices on Transparency in Fiscal Policy	EN
Effective Insolvency and Creditor Rights Systems	II
International Financial Reporting Standards	ID
Principles of Corporate Governance	EN
International Standards on Auditing	ID
Anti-Money Laundering/Combating Terrorist Financing Standard	ID
Core Principles for Systemically Important Payment Systems	ID
Core Principles for Effective Banking Supervision	EN
Objectives and Principles of Securities Regulation	ID
Insurance Core Principles	ID

II = Insufficient Information | NC = No Compliance | ID = Intent Declared | EN = Enacted | CP = Compliance in Process | FC = Full Compliance

source: http://estandardsforum.org/indonesia/standards

Level of Compliance

Full Compliance	10 points
Compliance in Progress	8 points
Enacted	6 points
Intent Declared	3 points
No Compliance	1 points
Insufficient Information	0 points

Compliance Factor

Indicator	Best Practice Benchmark	Points
1. Economic Model	Market-based economy	1 point
2. FOREX Regulations	No Capital Controls	1/2 point
	No Exchange Controls	1/2 point
3. Foreign Investment Law	Yes, adequate Foreign Investment Law	1 point
4. Trade Regulation	No Import Regulation	1/4 point
	No Protective Tariffs	1/4 point
	Yes, Export Incentives	1/4 point
	No Export Disincentives	1/4 point
5. Tax Regime	Creates Incentives for Investment	1 point
6. Tax Rates	Low / Competitive	1 point
7. Bankruptcy Indicators/ Property Rights	Established	1 point
8. International Dispute Settlement	Credible History/Marginal Success	1 point
9. Political Environment	Positive Commitment to globalism by ruling authority	1/3 point
	Positive Attitude toward utilization of global resources to promote growth	1/3 point
	Positive Commitment to globalism by political opposition	1/3 point
10. Political Stability	Yes, for foreseeable future	1 point
11.Corruption	No Concern	1 point
12. Adherence to global labor standards	Complies	1 point