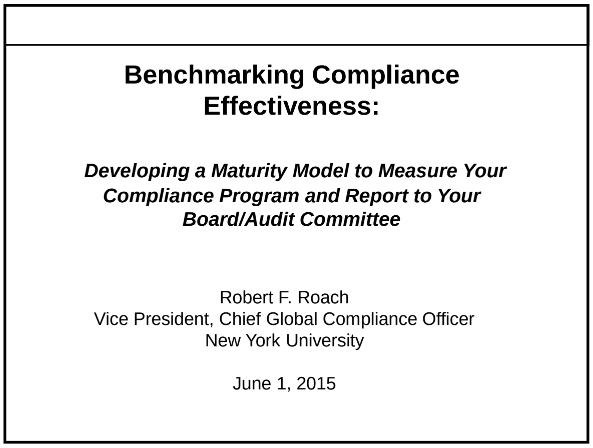
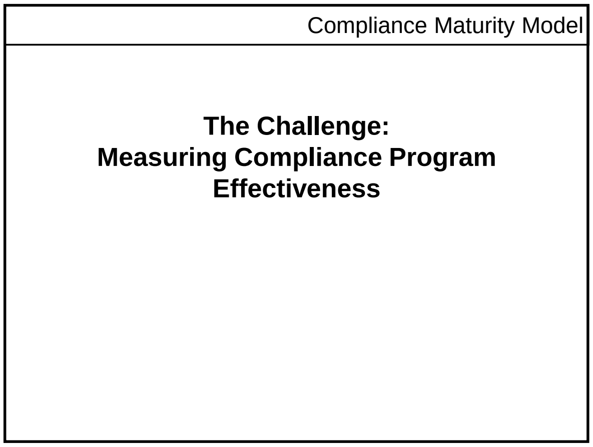


Benchmarking Compliance Effectiveness:

Developing a Maturity Model to Measure Your Compliance Program and Report to Your Board/Audit Committee

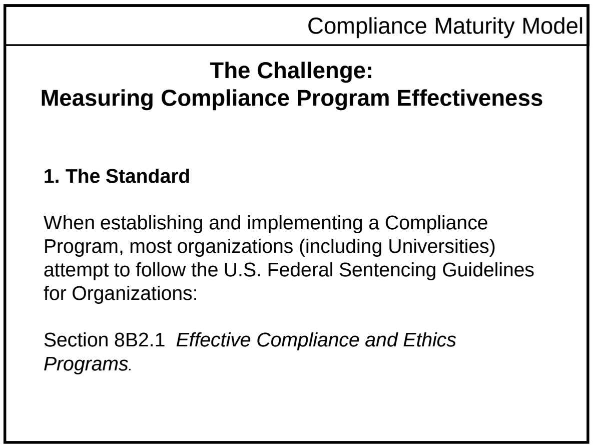
Robert F. Roach
Vice President, Chief Global Compliance Officer
New York University

June 1, 2015



Compliance Maturity Model

The Challenge: Measuring Compliance Program Effectiveness



Compliance Maturity Model

The Challenge: Measuring Compliance Program Effectiveness

1. The Standard

When establishing and implementing a Compliance Program, most organizations (including Universities) attempt to follow the U.S. Federal Sentencing Guidelines for Organizations:

Section 8B2.1 *Effective Compliance and Ethics Programs*.

Compliance Maturity Model

2. The Guidelines don’t always help!

While the Guidelines set forth basic elements of an effective compliance program, they make clear that:

- No single compliance program design fits every organization.
- An organization's industry, size, structure and mission all influence program design and operation.

3. The Challenge:

The Guidelines direct us to have an “effective” program, but how do you define and measure the effectiveness of your Compliance program?

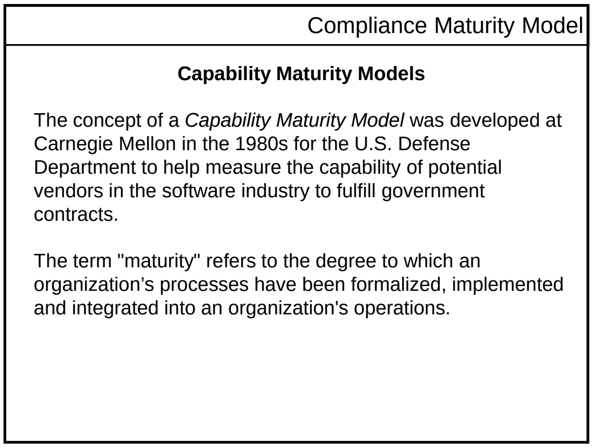
Compliance Maturity Model

4. Practical Issues

- Easier to track program activities than results
- Difficult to determine which compliance activities drive results
- Difficult to assess employee and management behavior objectively and consistently over time
- Lack of useful benchmarks for comparison
- Often difficult to glean actionable information from self assessments

Compliance Maturity Model

Capability Maturity Models

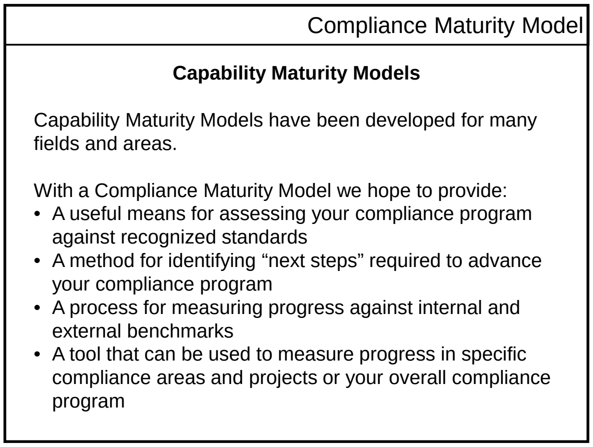


Compliance Maturity Model

Capability Maturity Models

The concept of a *Capability Maturity Model* was developed at Carnegie Mellon in the 1980s for the U.S. Defense Department to help measure the capability of potential vendors in the software industry to fulfill government contracts.

The term "maturity" refers to the degree to which an organization’s processes have been formalized, implemented and integrated into an organization's operations.



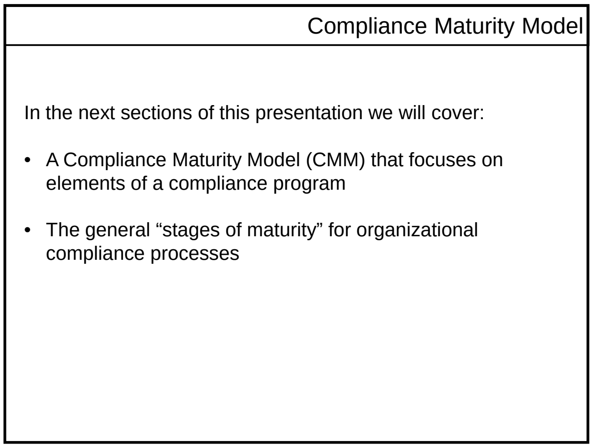
Compliance Maturity Model

Capability Maturity Models

Capability Maturity Models have been developed for many fields and areas.

With a Compliance Maturity Model we hope to provide:

- A useful means for assessing your compliance program against recognized standards
- A method for identifying “next steps” required to advance your compliance program
- A process for measuring progress against internal and external benchmarks
- A tool that can be used to measure progress in specific compliance areas and projects or your overall compliance program



Compliance Maturity Model

In the next sections of this presentation we will cover:

- A Compliance Maturity Model (CMM) that focuses on elements of a compliance program
- The general “stages of maturity” for organizational compliance processes

Compliance Maturity Model

A Compliance Maturity Model (CMM)

Compliance Maturity Model

Compliance as an Afterthought:

Many organizations have "bolted on" compliance programs that are separate and apart from their "business" operations. They have not integrated a focus on compliance risk management within operational and decision making processes.

The overall results are fragmented compliance programs that are complicated to operate and difficult to coordinate, manage, and monitor. These systems also tend to be reactive rather than planned or strategic.

Compliance Maturity Model

CMM Maturity Levels

A CMM focuses on integration of your compliance programs into organizational business processes by analyzing the "maturity" of your program with levels that range from *ad hoc* practices, to formally defined steps, to managed with result metrics, to active optimization of processes. As an organization moves up the maturity model, ownership spreads across the organization and becomes embedded within the very culture of the organization.

Note: capability maturity models vary in the number of "maturity" levels they use – usually three to five. They also use somewhat different descriptive labels. We have developed a CMM with five levels and the most frequently used labels for maturity levels.

Compliance Maturity Model

*1. **Ad Hoc**: Procedures are usually informal, incomplete and inconsistently applied.*

*2. **Fragmented:** There are some compliance controls in place, but they are not consistent across the organization. Often limited to certain areas or managed in "silos" (e.g. EHS, Finance, Research, etc.)*

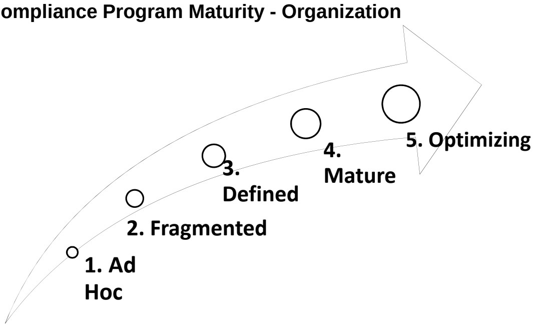
*3. **Defined**: Compliance Controls and procedures are documented and standardized across the organization*

*4. **Mature**: Compliance procedures are an integral part of business processes and periodic reviews are conducted to access effectiveness of the program*

*5. **Optimized**: Regular review and feedback are used to ensure continuous improvement towards optimization of compliance processes; elements are often automated, which are more effective at preventing compliance failures and ultimately less costly than manual controls focusing on detection*

Compliance Maturity Mode - Organization

Compliance Program Maturity - Organization



1. Ad Hoc

2. Fragmented

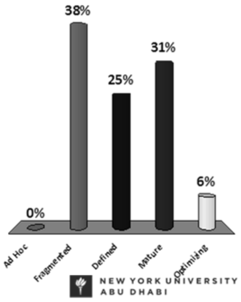
3. Defined

4. Mature

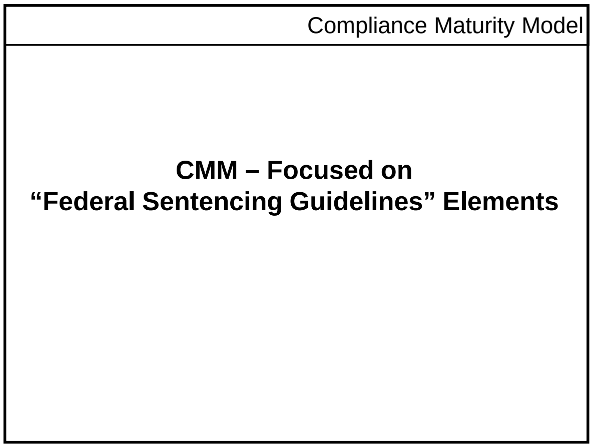
5. Optimizing

Compliance Program Maturity - Organization

A. Ad Hoc
B. Fragmented
C. Defined
D. Mature
E. Optimizing

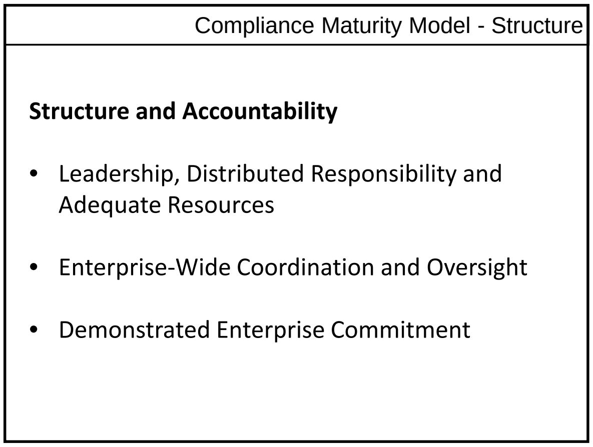


NEW YORK UNIVERSITY ABU DHABI



Compliance Maturity Model

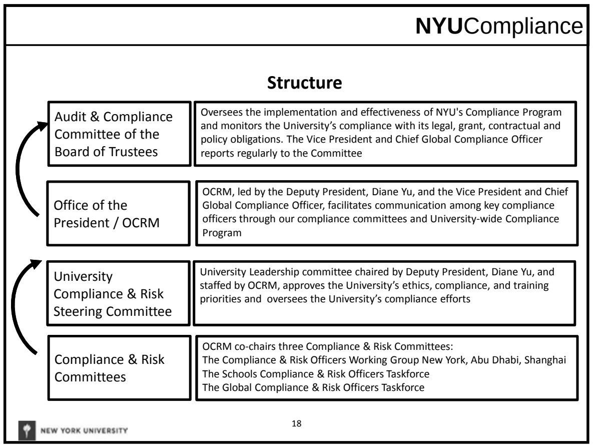
CMM – Focused on “Federal Sentencing Guidelines” Elements



Compliance Maturity Model - Structure

Structure and Accountability

- Leadership, Distributed Responsibility and Adequate Resources
- Enterprise-Wide Coordination and Oversight
- Demonstrated Enterprise Commitment



NYUCompliance

Structure

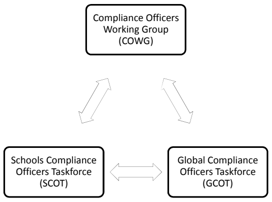
Audit & Compliance Committee of the Board of Trustees	Oversees the implementation and effectiveness of NYU's Compliance Program and monitors the University’s compliance with its legal, grant, contractual and policy obligations. The Vice President and Chief Global Compliance Officer reports regularly to the Committee
Office of the President / OCRM	OCRM, led by the Deputy President, Diane Yu, and the Vice President and Chief Global Compliance Officer, facilitates communication among key compliance officers through our compliance committees and University-wide Compliance Program
University Compliance & Risk Steering Committee	University Leadership committee chaired by Deputy President, Diane Yu, and staffed by OCRM, approves the University’s ethics, compliance, and training priorities and oversees the University’s compliance efforts
Compliance & Risk Committees	OCRM co-chairs three Compliance & Risk Committees: The Compliance & Risk Officers Working Group New York, Abu Dhabi, Shanghai The Schools Compliance & Risk Officers Taskforce The Global Compliance & Risk Officers Taskforce

NEW YORK UNIVERSITY

18

NYUCompliance

OCRM Compliance Committees


Compliance Officers Working Group (COWG)
Schools Compliance Officers Taskforce (SCOT)
Global Compliance Officers Taskforce (GCOT)

COWG: includes compliance officers from academic and administrative departments, including NYU Abu Dhabi, who are responsible for day to day compliance activities. COWG currently has a membership of more than 25 compliance officers.

SCOT: includes representatives appointed by the deans and directors of all of NYU's Schools, Colleges and major Institutes, including NYU Poly and the Center for Urban Science and Progress (CUSP). SCOT was formed in 2012 as a forum for Schools to discuss their unique compliance concerns and as a vehicle to enhance compliance communication with COWG and GCOT.

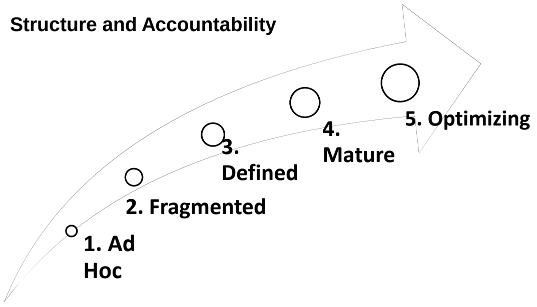
GCOT: provides a forum for administrators at Washington Square who have responsibilities for the academic and administrative development at the Global Sites.

Compliance Maturity Model - Structure

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
There is no formal compliance structure	Senior management and Board discourage noncompliance but not consistent in follow through	A compliance structure has been established, with accountability assigned to key risk area officers	Compliance risk assessments and mitigation plans are completed by risk area officers on a regular, timely and consistent basis	Network of compliance officers representing every significant operation in place and they meet regularly to coordinate compliance activities
No Independent oversight	Accountability is broadly understood but not formally documented. Oversight and monitoring are inconsistent	Senior Compliance Committee exists, includes representatives of key organizational activities	Reporting by risk area officers to Chief Compliance Officer is timely and consistent	Senior Compliance Committee considers compliance a strategic priority. Compliance risk scenarios have been identified, assessed and mapped to compliance controls, which are updated at least annually.
Accountability is not defined	Senior compliance committee may exist, but compliance activities reactive and in silos	Chief Compliance Officer or other individual with day to day responsibility for compliance appointed	The senior compliance committee meets at least quarterly, receives regular reports by Chief Compliance Officer, actively plans for compliance contingencies	The Board/Audit Committee and executive management show a demonstrated commitment to compliance throughout the organization.
Compliance risks are not understood	Compliance risks are understood but not formally documented.	Process in place for identifying compliance risks and developing mitigation plans by assigned risk area officers	Chief Compliance Officer has independent and direct access to Board or Audit Committee. Makes regular reports on compliance activities to Board/Audit Committee.	Compliance, risk management and internal audit have implemented integrated work plans. Integrated functions are supported by automated processes.

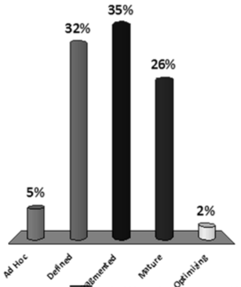
Compliance Maturity Model - Structure

Structure and Accountability



Structure and Accountability

A. Ad Hoc
B. Defined
C. Fragmented
D. Mature
E. Optimizing



NEW YORK UNIVERSITY ABU DHABI

Compliance Maturity Model - Policies

Policies and Procedures

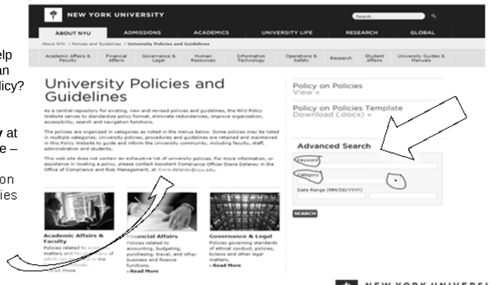
- Distributed and Assigned Responsibility
- Development and Publication
- Accessibility and Communication
- Policy Tracking, Review and Maintenance

NYUCompliance

www.nyu.edu/policies

*User-friendly! Search by **keyword**, **category** or date range*

Need help finding an NYU policy? Contact **Diane Delaney** at our office – Diane's email is on the poicies page



University Policies and Guidelines

As a central repository for existing, new and revised policies and guidelines, the NYU Policy Website serves to standardize policy format, eliminate redundancies, improve organization, accessibility, search and navigation functions.

The policies are organized in categories as noted in the menus below. Some policies may be listed in multiple categories. University policies, procedures and guidelines are retained and maintained in this Policy Website to guide and inform the University community, including faculty, staff, administration and students.

This web site does not contain an exhaustive list of university policies. For more information, or assistance in locating a policy, please contact Assistant Compliance Officer Diane Delaney in the Office of Compliance and Risk Management, at diane.delaney@nyu.edu.

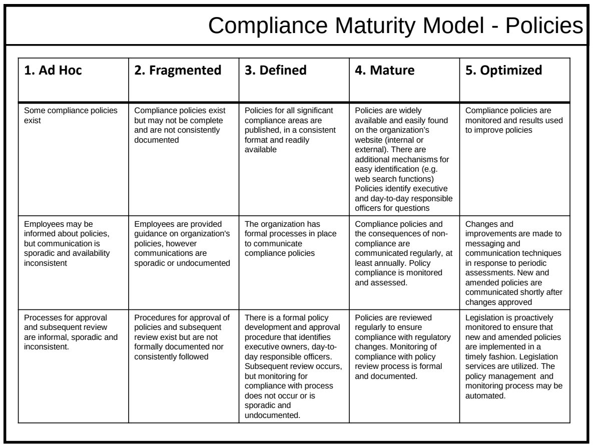
Academic Affairs & Faculty
Policies related to academic matters and faculty, many of which can be found in the Faculty Handbook.
» Read More

Financial Affairs
Policies related to accounting, budgeting, purchasing, travel, and other business and finance functions.
» Read More

Governance & Legal
Policies governing standards of ethical conduct, policies, bylaws and other legal matters.
» Read More

NEW YORK UNIVERSITY

NEW YORK UNIVERSITY ABU DHABI 24

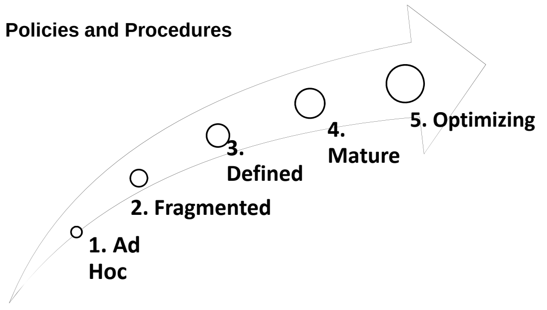


Compliance Maturity Model - Policies

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Some compliance policies exist	Compliance policies exist but may not be complete and are not consistently documented	Policies for all significant compliance areas are published, in a consistent format and readily available	Policies are widely available and easily found on the organization's website (internal or external). There are additional mechanisms for easy identification (e.g. web search functions) Policies identify executive and day-to-day responsible officers for questions	Compliance policies are monitored and results used to improve policies
Employees may be informed about policies, but communication is sporadic and availability inconsistent	Employees are provided guidance on organization's policies, however communications are sporadic or undocumented	The organization has formal processes in place to communicate compliance policies	Compliance policies and the consequences of non-compliance are communicated regularly, at least annually. Policy compliance is monitored and assessed.	Changes and improvements are made to messaging and communication techniques in response to periodic assessments. New and amended policies are communicated shortly after changes approved
Processes for approval and subsequent review are informal, sporadic and inconsistent.	Procedures for approval of policies and subsequent review exist but are not formally documented nor consistently followed	There is a formal policy development and approval procedure that identifies executive owners, day-to-day responsible officers. Subsequent review occurs, but monitoring for compliance with process does not occur or is sporadic and undocumented.	Policies are reviewed regularly to ensure compliance with regulatory changes. Monitoring of compliance with policy review process is formal and documented.	Legislation is proactively monitored to ensure that new and amended policies are implemented in a timely fashion. Legislation services are utilized. The policy management and monitoring process may be automated.

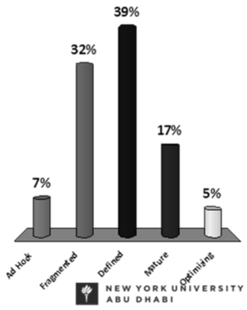
Compliance Maturity Model - Policies

Policies and Procedures



Policies and Procedures

A. Ad Hock
B. Fragmented
C. Defined
D. Mature
E. Optimizing



NEW YORK UNIVERSITY
ABU DHABI

Compliance Maturity Model –Training/Communication

Training and Communication

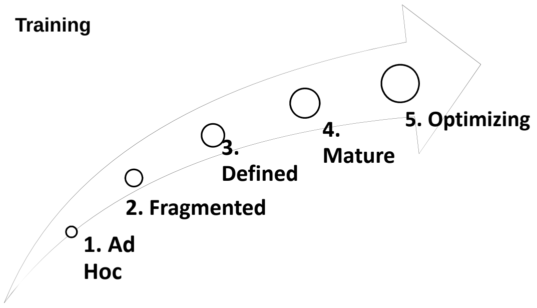
- Planning and Content
- Distributed and Assigned Responsibilities
- Delivery Mechanisms (In-person, Online, Automation)
- Audience – Needs Identification
- Audit Trail, Tracking and Metrics
- Assessment and Certification

Compliance Maturity Model - Training

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Formal compliance training is not provided. However, compliance information may be communicated by informal means	The organization provides compliance training but it is sporadic or in silos.	Compliance training is provided throughout the organization as needed in a scheduled and timely fashion. Training metrics may not be collected and reported to executives or the Board in a regular or consistent fashion.	An enterprise wide compliance training program exists and is monitored by management/responsible officers. The organization identifies persons needing training in key compliance areas and monitors their participation. Training metrics are collected and reported to executives and the Board. At least annually.	A program of compulsory compliance training is implemented. Automation is used in program delivery and monitoring. Competency assessments and certification programs are implemented in key compliance areas. Monitoring and metrics are used to continuously improve training.
There is no formal compliance communication program.	Occasional communication about compliance may occur, but it is sporadic and informal	Compliance communications such as newsletters, email blasts, posters and other methods used. There is no formal documented compliance communication program.	The organization has developed a formal compliance communication plan that is documented and updated at least annually.	Compliance monitoring and metrics are used to continuously improve the compliance communication plan.

Compliance Maturity Model

Training

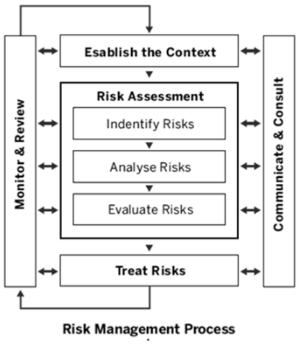


Compliance Maturity Model – Risk

Risk Assessment

- Process – Defined Formal Methodology
- Distributed Responsibility and Ownership
- Scope – Complete and Enterprise-Wide
- Risk Criteria
- Mitigation Plans
- Monitoring – Responsible Officers and Independent
- Reporting and Oversight

Compliance Maturity Model – Risk

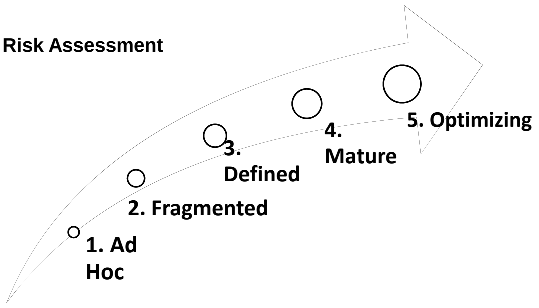


Compliance Maturity Model - Risk

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Compliance Risks may have been identified, but not the result of any formal process	Employees may be aware of and consider various compliance risks.	Processes have been implemented for risk identification, assessment and reporting .	All formal processes for compliance risk management have been implemented throughout the organization and are formally documented through a risk register or other means.	Compliance, Risk Management and Internal Audit have integrated risk management processes that are improved continuously through ongoing monitoring. Risks customized by jurisdiction.
A compliance risk assessment has not likely been completed and risk formally documented	Risk assessments may not be conducted regularly, but are not part of a regular risk management program and may not cover all areas.	A formal risk management processes has been adopted, such as ISO 31000 or COSO ERM.	All risks are assessed at least annually. Mitigation plans are monitored by risk owners and reviewed by independent department (e.g. compliance or internal audit)	Executive management and Board regularly review risk program and provide leadership for key strategic and institutional risks.
			Results of risk management process at least annually to executive management and Board.	Automation for risk management process may be implemented.

Compliance Maturity Model - Risk

Risk Assessment



1. Ad Hoc

2. Fragmented

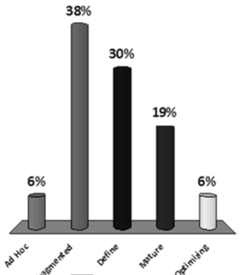
3. Defined

4. Mature

5. Optimizing

Risk Assessment

A. Ad Hoc
B. Fragmented
C. Define
D. Mature
E. Optimizing



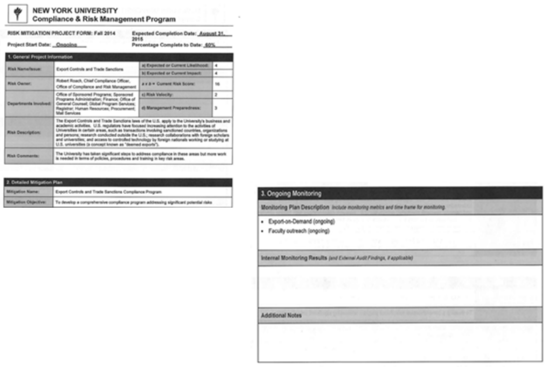
NEW YORK UNIVERSITY ABU DHABI

Compliance Maturity Model - Monitoring

Monitoring

- Standards
- Ownership – Distributed and Independent
- Remedial Action Plans
- Metrics
- Reporting and Oversight

Compliance Maturity Model - Monitoring



NEW YORK UNIVERSITY
Compliance & Risk Management Program

RISK MITIGATION PROJECT FORM: Fall 2014 — Expected Completion Date: August 31, 2015

Project Start Date: Ongoing — Percentage Complete to Date: 60%

1. General Project Information			
Risk Name/Issue:	Export Controls and Trade Sanctions	a) Expected or Current Likelihood:	4
		b) Expected or Current Impact:	4
Risk Owner:	Robert Roach, Chief Compliance Officer, Office of Compliance and Risk Management	a x b = Current Risk Score:	16
Departments Involved:	Office of Sponsored Programs; Sponsored Programs Administration; Finance; Office of General Counsel; Global Program Services; Registrar; Human Resources; Procurement; Mail Services	c) Risk Velocity:	2
		d) Management Preparedness:	3
Risk Description:	The Export Controls and Trade Sanctions laws of the U.S. apply to the University's business and academic activities. U.S. regulators have focused increasing attention to the activities of Universities in certain areas, such as transactions involving sanctioned countries, organizations and persons; research conducted outside the U.S.; research collaborations with foreign scholars and universities; and access to controlled technology by foreign nationals working or studying at U.S. universities (a concept known as "deemed exports").		
Risk Comments:	The University has taken significant steps to address compliance in these areas but more work is needed in terms of policies, procedures and training in key risk areas.		

2. Detailed Mitigation Plan	
Mitigation Name:	Export Controls and Trade Sanctions Compliance Program
Mitigation Objective:	To develop a comprehensive compliance program addressing significant potential risks

3. Ongoing Monitoring

Monitoring Plan Description *Include monitoring metrics and time frame for monitoring*

- Export-on-Demand (ongoing)
- Faculty outreach (ongoing)

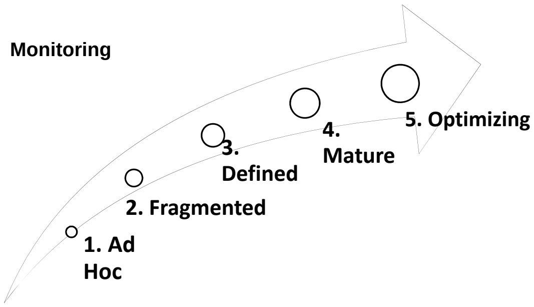
Internal Monitoring Results *(and External Audit Findings, if applicable)*

Additional Notes

Compliance Maturity Model - Monitoring

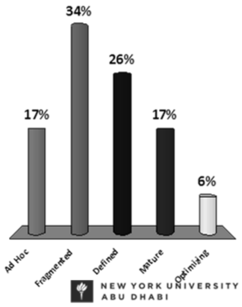
1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Monitoring of compliance program elements and risks are informal and ad hoc.	Monitoring of compliance program elements and risks exist but may not cover all all aspects	Monitoring of compliance program cover all relevant elements and risks.	Monitoring of compliance cover all program elements and risks.	Monitoring is coordinated and integrated into Compliance, IA and Risk Management Functions.
Guidance on monitoring is not formally provided or documented	Some guidance provided but not fully documented.	Monitoring is fully documented.	Monitoring is fully documented and includes both ongoing monitoring by risk owners and independent monitors (e.g. compliance officer or IA)	Formal integrated monitoring plans are developed at least annually by Compliance, IA and Risk Management. Monitoring plans are reviewed and approved at least annually by executives and Board.
			Monitoring results with corrective action plans are reported to executives and Board	Metrics arising from monitoring activities are developed, reported and utilized to drive continuous improvement in the Compliance Program. Automation is used when possible.

Compliance Maturity Model - Monitoring



Monitoring

A. Ad Hoc
B. Fragmented
C. Defined
D. Mature
E. Optimizing



NEW YORK UNIVERSITY
ABU DHABI

Compliance Maturity Model

Projects and Deep Dives

Compliance Maturity Model

Projects and Deep Dives

- Specific Compliance Processes
  - *Compliance Complaint Processes*
- Specific Compliance Subject Matters
  - Privacy
- Compliance Program Qualities/Results
  - Compliance Culture
- Department or Compliance Function
  - Human Subjects Research

Compliance Maturity Model

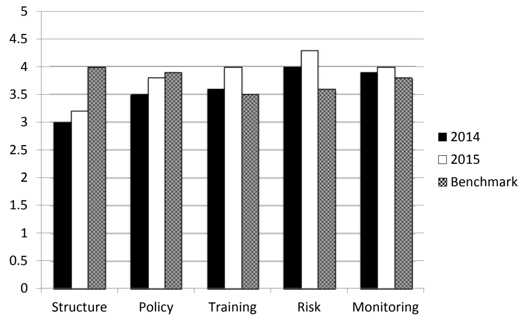
Reporting CMM to the Board:
By Compliance Program Element

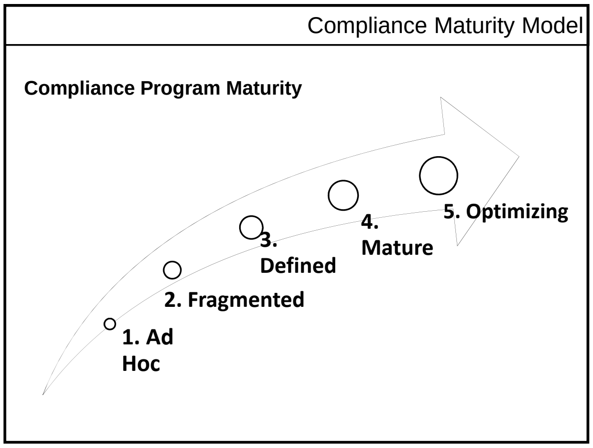
Compliance Maturity Model

**Reporting CMM to the Board:
By Compliance Program Element**

- Snapshot by Element
- By Target or Goal
- Year-on-Year Comparison
- Benchmarking

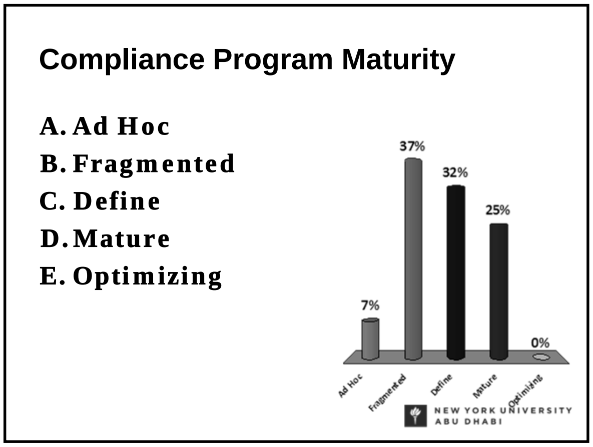
Compliance Maturity Model





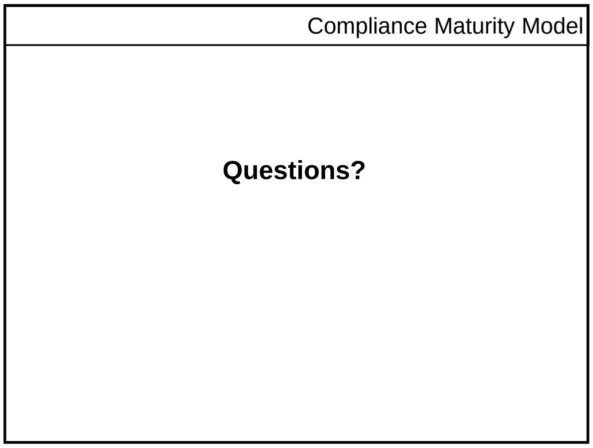
Compliance Maturity Model

Compliance Program Maturity



Compliance Program Maturity

- A. Ad Hoc
- B. Fragmented
- C. Define
- D. Mature
- E. Optimizing



Compliance Maturity Model

Questions?