ISO 37001 ANTI-BRIBERY MANAGEMENT SYSTEM FOUNDATION

Overview & Obtaining Benefits from the New Standard

Abidjan: March 26, 2019

Introductions

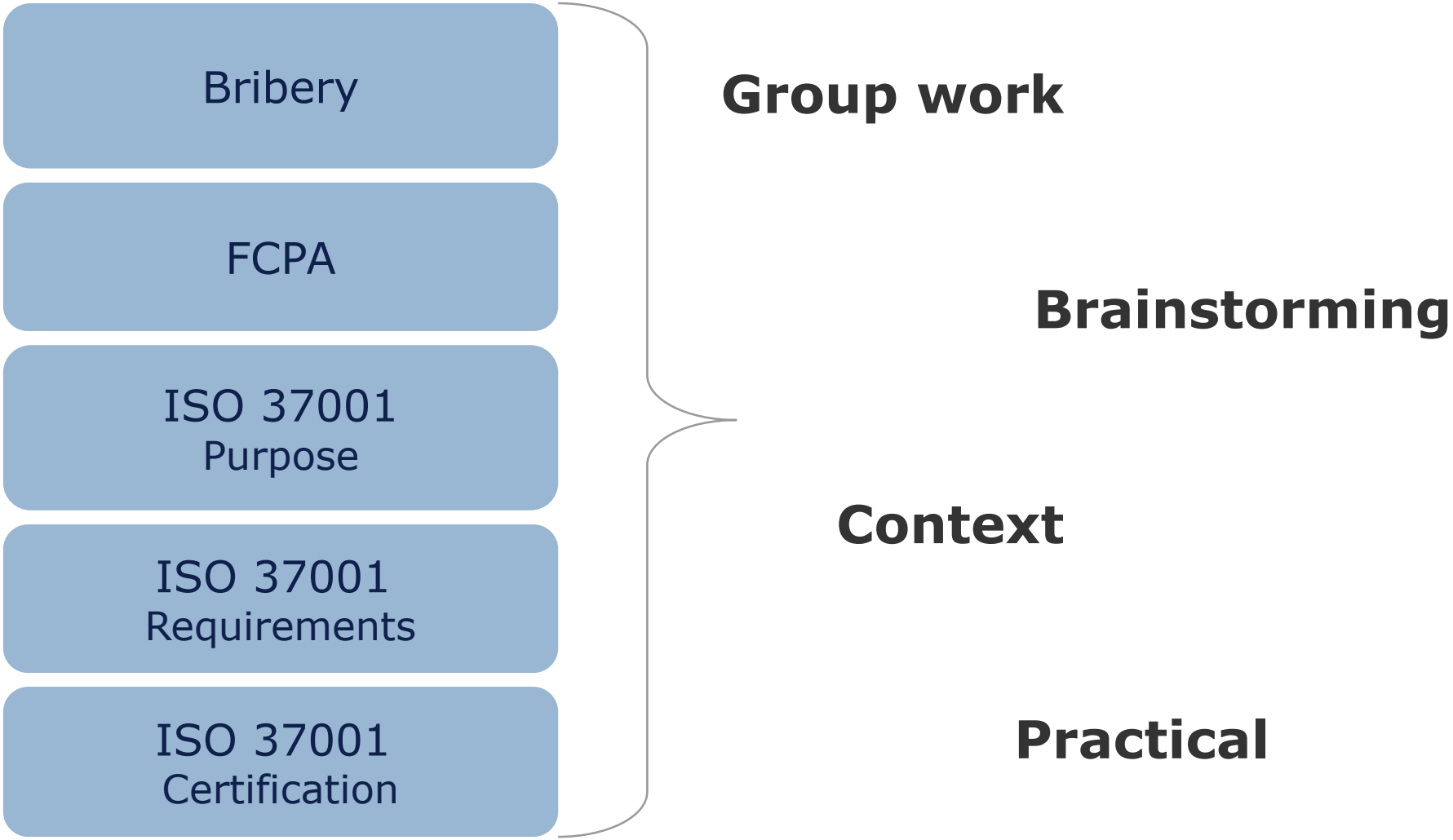
- Meet and interview the person next to you.
- Find out, record and be ready to present your colleague's:
  - Name
  - Organization and role in the organization
  - Experience with anti-bribery and anti-corruption practice and theory
  - Expectations from this training course
  - Interesting fun-fact

5 minutes

Our Learning Objectives for this Course

- What is bribery – and how does it affect us?
- What is the Foreign Corrupt Practices Act (FCPA) – and what is its impact?
- What is the ISO 37001 Anti-bribery Management Systems standard?
  - Why was it created?
  - How is the standard different from the FCPA?
  - What are its benefits?
- How does ISO 37001 work?
  - What is/are its structure, contents, principles and key concepts?
- How does an organization prepare for an ISO 37001 certification audit?

How This Course is Structured



How to contribute today

Learning new things is demanding, but fun

Active participation

There are no stupid questions

Benefit from sharing experiences

Class Administration

- In case of fire
- Restrooms
- Electronics
- Breaks
- *Anything else?*

What is ISO 37001?

- A management system for the ***detection*** and ***prevention*** of bribery
  - Business processes supporting (voluntary) business and (mandatory) legal anti-bribery goals and objectives
- Developed by global organizations to help small, medium and large organizations (private sector, governments and others) to:
  - Establish,
  - Manage, and
  - Continuously improve an anti-bribery management systems (ABMS)
  - Certification and associated ***strategic benefits***
  - Recognition for compliance – UP FRONT!!!
  - Tangible indication of voluntarily "going above and beyond"
  - Differentiator in the market for competitive bids (e.g. RFPs and RFQs)
    - Message: I'm a better partner choice – I've taken affirmative steps to reduce a high risk

A visual summary of ISO 37001's steps

Risk assessment

- Stakeholder mapping
- Context
- Gap analysis
- Workshops
- Risk register

Strategy

- Set target
- Decide priorities
- Budget

Governance & management system

- Policies and procedures
- Implementation plans (controls)
- Roles and responsibilities

Training & awareness

- Training program
- Roll out and implementation
- Effect

Assess and check implementation

- Management reporting
- Audits
- (Wh…

Review and continuous improvement

- Regular management review
- Result vs. …and
- …sons

1. What is Bribery ?

2. What is the FCPA?

3. What is ISO 37001?

4. How does ISO 37001 work?

5. How do I prepare for an ISO 37001 audit?

Together we will cover…

- Forms of bribery
- Size and aspects of the problem – including effects on us
- Why hasn't more been done about it?

Recent ISO 37001 developments

- ***Large US companies:***
  - Microsoft and Walmart announcements, Legg Mason certification
- ***Non-US companies' certifications:***
  - Alstom – France
  - Edesur – Argentina
  - Many Brazilian and Italian firms
- ***Adoption by various governments:***
  - Peru, Indonesia, Singapore, UAE
  - Montreal, Shenzhen
  - Under review in Nigeria
- ***Recognition by anti-bribery law enforcement:***
  - Brazil – Odebrecht settlement
  - Denmark – Atea Denmark

What is Bribery? - The Details

- Can take **various forms**
- **Foreign Corrupt Practices Act (FCPA)**:
  - US law – enforced by Dept. Of Justice
  - Focus: Providing or offering anything of value to a foreign governmental official for the purposes of obtaining or retaining business
- **Cultural factors** - what's normal and customary in one place (e.g. Diwali gifts in India) may be unknown in others
- **Economic factors** –in many places overseas, governmental officials can't support families on salaries

How big is the problem? (The Macro View)

- **Globally (World Bank - 2017)**
  - $2 T per year: bribes by companies/individuals
  - 2% of global GNP
  - Non-financial impact to democratic institutions (rule of law)
- **US (FBI – 2018)**
  - Billions lost annually: public corruption
  - Overseas and domestic corruption in all forms is a threat to:
    - National security
    - Free markets
    - Democracy

International Anti-Bribery/Anti-Corruption Initiatives

- Business For Social Responsibility (1992)
- Transparency International (1993)
- The World Business Council For Sustainable Development (1995)
- OECD Convention Against Corruption (1999)
- Global Reporting Initiative (2002; GRI G4 56-58)
- UN Convention Against Corruption (2003)
- The Extractive Industries Transparency Initiative (2003)
- UN Global Compact´s 10th Principle (2005)
- The Principles for Responsible Investment (2006)
- The Principles for Responsible Management Education (2007)
- The International Integrated Reporting Council (2010)

Impact 1: The Problem with Bribery

- Discuss within your group:
  - How does bribery affect me – personally and/or professionally?
  - What are the ways that my organization could prevent bribery from adversely affecting our operations and financial results?

10 minutes

Reflection – we have covered…

- Forms of bribery
- Size and aspects of the problem – including effects on us
- Why hasn't more been done about it?

1. What is Bribery ?

2. What is the FCPA – the leading anti-bribery legal standard?

3. What is ISO 37001?

4. How does ISO 37001 work?

5. How do I prepare for an ISO 37001 audit?

Together we will cover…

- What is Bribery ?
  - It matters…
- What is the FCPA?
  - It's the "law of the land" and costs/penalties of non-compliance are high, but difficult to interpret, costly to apply and no compliance validation
- What is ISO 37001 – Anti-bribery management systems?
  - Business response: to help support and demystify anti-bribery

FCPA Focus Areas

1. **Anti-bribery Component:** Prohibits bribery (both the offer and the payment) and non-routine payments ("anything of value") to *foreign governmental officials*

   "…any officer or employee of a foreign government or any department, agency, or instrumentality thereof."

   *** and ***

2. **Financial Record Keeping & Internal Control Component:** Requires precise records and financial internal controls to be maintained to provide reasonable assurance of accuracy of financial records and to demonstrate compliance

   "Books and records provisions"

FCPA Enforcement Agencies

Department of Justice (DOJ)	• Criminal enforcements • Some civil actions - against non-issuers
Securities and Exchange Commission (SEC)	• Civil actions against issuers (public co's)

USA (DOJ and SEC)

- 1. **Petrobras** (Brazil): $1.73 Bi (2018)
- 2. **Telia Company AB** (Sweden): $965 million (2017)
- 3. **Siemens** (Germany): $800 million (2008)
- 4. **VimpelCom** (Holland) $795 million (2016)
- 5. **Alstom** (France): $772 million (2014)
- 6. **Société Générale S.A.** (France): $585 million (2018)
- 7. **KBR / Halliburton** (United States): $579 million (2009)
- 8. **Teva Pharmaceutical** (Israel): $519 million (2016)
- 9. **Keppel Offshore & Marine Ltd.**(Singapore): $422 million (2017)
- 10. **Och-Ziff** (United States): $412 million (2016)

UK

- Tesco (UK): £129m (2017)
- Rolls Royce (UK, US, Brazil): £497m (plus $170m US and $25m Brazil) (2017)
- XYZ (UK, not settled yet): £6.5m (2016)
- Braid Group (Scotland): £2.2m (2016)
- Sweet Group (UK): £1.4m (2016)
- Standard Bank (UK): £26m (2015)

FCPA

- ***Trends:***
  - Prosecution of individuals is a priority
  - Settlement amounts continue to increase
  - Cooperation/coordination with overseas law enforcement continues to improve
  - Case law and enforcement practices continue to evolve
    - FCPA Guidance (2013)
    - FCPA Policy (2017)
- ***Realities:***
  - FCPA is a powerful, profitable tool for US government
    - Enforcement historically favored by both parties
    - Perceived as supporting democratic values:
      - Free market
      - Rule of law

Business's Frustrations with the FCPA

- "Thou shalt not…" – what NOT to do
- Ambiguous, opaque and changing standards- e.g. definition of "governmental official"
- Costly compliance with uncertain ROI
- How do I know if I have a good program?
  - The PROCESS IS "BACK-END LOADED": PROGRAM "EFFECTIVENESS" IS DETERMINED ONLY AFTER CONSIDERABLE TIME (OFTEN YEARS) AND COST (E.G. MANAGEMENT TIME, PROFESSIONAL FEES) spent on an investigation
- Unsympathetic regulators/enforcers
  - Recent (more positive) changes with DOJ under Atty. Gen. Sessions

Other Law: UK Bribery Act & Sapin II

- **UK: Strict liability violation: failure of commercial organizations to prevent bribery**

  A commercial organization (with UK ties) is guilty of an offense if a person associated with the organization bribes another person with the intention of either

  - Obtaining or retaining business for the organization, or
  - Obtaining or retaining an advantage in the conduct of business for the organization

- Defense, however, if the organization can show that it has put in place **adequate procedures** designed to prevent persons associated with the organization from undertaking corrupt activities
- **FRANCE: Requirement for companies over a certain size (employees and revenues) to have an 8-point anti-corruption compliance program in place**
  - Adoption of leading law enforcement practices

Impact 2: A Better Way to Fight Bribery

- Discuss within your group:
  - ***What would "better guidance" on managing the risks of bribery look like?***
    - ***What components would it have?***
    - ***What would it require?***
- Keep track of your ideas and be prepared to present to the class.

15 Minutes

Reflection – we have covered…

- What is Bribery ?
  - It matters…
- What is the FCPA, UKBA and Sapin II?
  - It's the "law of the land" and costs/penalties of non-compliance are high, but difficult to interpret, costly to apply and no compliance validation
- What is ISO 37001 – Anti-bribery management systems?
  - Business (non-legal world) response: to help support and demystify anti-bribery

1. What is Bribery ?

2. What is the FCPA?

3. What is ISO 37001?

4. How does ISO 37001 work?

5. How do I prepare for an ISO 37001 audit?

Together we will cover…

- ISO
- ISO 37001 creation
- Practical differences between FCPA and ISO 37001
- Benefits of ISO 37001 certification:
  - Operating
  - Strategic
- Other high level aspects of the standard

About ISO

- Independent, non-governmental, non-profit international organization based in Geneva, Switzerland
- Membership: 161 national standards bodies
- Brings together experts to share knowledge and develop voluntary, consensus-based, market relevant international standards

Needs-driven

Supports innovation and global trade

Provides structure and process

About ISO standards

- International Standards **make things work**
  - World-class ISO specifications operate largely "behind the scenes" for products, services and systems - to ensure quality, safety and efficiency - facilitating **international trade**
- ISO has published 22205 International Standards and related documents, covering almost every industry, from technology, to food safety, to agriculture and healthcare
- ISO International Standards impact everyone, everywhere

A broader set of challenges…

Globalized supply chain and expectations of social responsibility

Rapid changes in competitive business landscape as well as in geo-political & environmental conditions

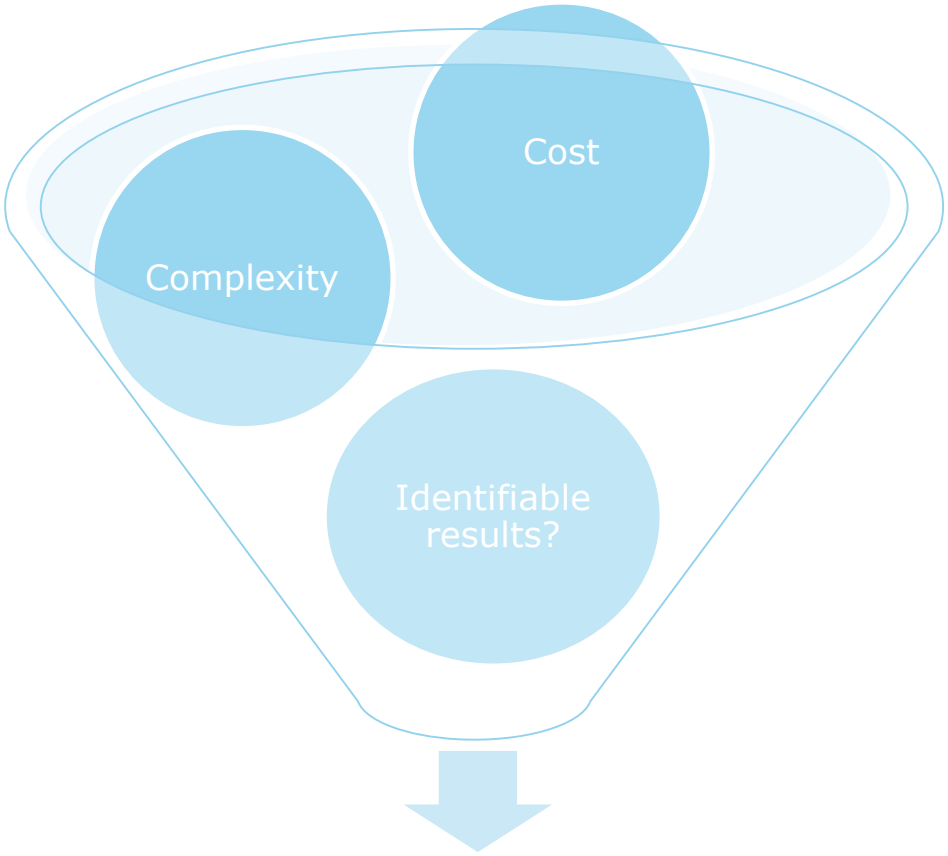
Sustainable business performance expected by investors, regulators, consumers and broader stakeholders (e.g. NGOs)

Transparency, accountability and independent assurance

Intangible assets as primary source of value (e.g. brand/reputation)

…demands a broader view.

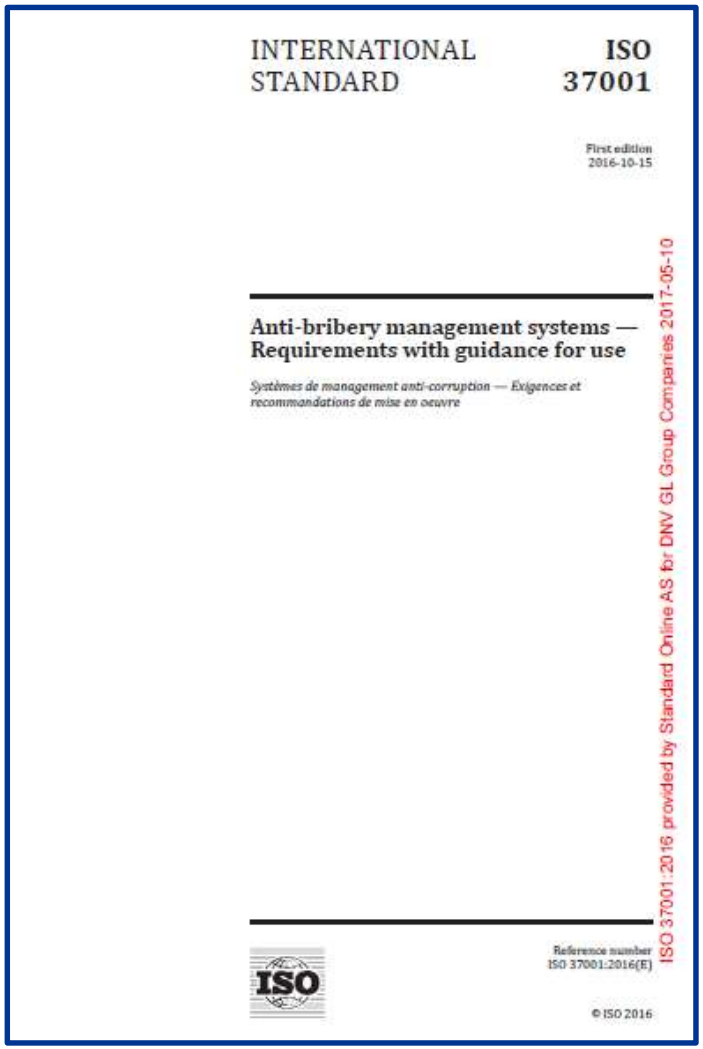
Why do we need an ISO-standard for anti-bribery?



Business (and non-US lawyer) perception: Anti-bribery "system" = ***BROKEN***

Creating the ISO 37001 ABMS standard

- 3+ years to develop and issue (after participating members vote)
- 37 countries directly participating: Australia, Austria, Brazil, Cameroon, Canada, China, Colombia, Croatia, Czech Republic, Denmark, Ecuador, Egypt, France, Germany, Guatemala, India, Iraq, Israel, Kenya, Lebanon, Malaysia, Mauritius, Mexico, Morocco, Nigeria, Norway, Pakistan, Saudi Arabia, Serbia, Singapore, Spain, Sweden, Switzerland, Tunisia, UK, USA, Zambia
- Cote d'Ivoire was an observing country
- US TAG (Technical Advisory Group) = 30+ members
  - Companies (e.g. Boeing, Microsoft)
  - Professional service firms (e.g. PwC, Deloitte)
  - Non-governmental organizations



What Are The Key Differences Between ISO 37001 and the FCPA?

- ***Testing the Effectiveness of the Program or System***
  - With **FCPA anti-corruption program**, the DOJ investigation/settlement process is "back-end loaded": "effectiveness" in a non-disclosure to DOJ scenario is determined after considerable time (years) and expenditure of professional fees
  - With **ISO 37001 anti-bribery management system** certification, the audit process establishes at the "front end" (and voluntarily) that the organization meets a rigorous anti-bribery standard based on an independent 3rd party audit
- ***Content and level of detail***
  - ISO 37001 provides "plain English" information on "what to do" and in many cases "how to do it". By contrast, legal standards are often ambiguous and generally focus on "what not to do".

Groups Who Benefit from ISO 37001

- **Governing Body:** improved oversight of top organizational risk area
  - How? ISO 37001 requires:
    - "ensuring that the organization's strategy and anti-bribery policy are aligned….receiving and reviewing information about the ABMS…requiring that adequate and appropriate resources needed for effective operation of the ABMS are allocated and assigned…." e.g. ***engagement*** (Sec. 5.1.1)
- **Top Management:** improved compliance "operationalization" and visibility
  - How? ISO 37001 requires:
    - "ensuring the integration of the ABMS requirements into the organization's processes… ensuring that the ABMS is appropriately designed to achieve its objectives… promoting an anti-bribery culture within the organization e.g. ***active involvement*** (Sec. 5.1.2)
- **Stakeholders** (citizens, shareholders, creditors, partners): greater bribery-risk management confidence = greater confidence in organization overall
  - Why? ISO 37001 certification = compliance with the standard as verified by an accredited and independent 3rd party (rigorous) on-site review process

Among the operating benefits provided by ISO 37001:

Common Language	• Leading practice anti-bribery processes and methodologies that are understood and function in different countries and jurisdictions
Efficiency	• Organizations and their supply chains can all operate under the same standard – instead of present case by case approach
Cost-savings	• Elimination of legal form focused positions (contract managers) • Opportunities to apply compliance personnel's skills to highest bribery risk operational risks

A Preview: What Certification Auditors Look For

What does an organization need to get certified (basic requirements)?

Reasonable, proportionate and risk-based policies, procedures and controls to prevent, detect and manage bribery, including, but not limited to:

- An anti-bribery policy including related procedures control functions
- Top management leadership, commitment and clear delegation of responsibility incl. oversight by a compliance manager or function
- Anti-bribery training (including the anti-bribery policy)
- Risk assessments and due diligence on projects and business associates
- Financial, procurement, commercial and contractual controls
- Reporting, monitoring, investigation, and review
- Documented corrective actions and continuous improvement

A Preview: Reasonable Assurance

On what basis is the certification provided by the certifying body (CB)?

- Based on review, testing and sampling
- Same standard as is applied to audit of a public company's financial statements by its CPA firm

  - e.g. Marriott International 2017 Form 10-K

  "REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

  …We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we *plan and perform the audit to obtain reasonable assurance* about whether the financial statements are free of material misstatement, whether due to error or fraud…"
- Not a guarantee
- Not based on exhaustive (and costly) deep dive (e.g. forensic investigative review)
- *Review cycle (both management and audit) needs to have occurred and be recurring*

Impact 3: Benefits for Your Organization

Discuss the following. Keep track of your ideas and be prepared to present to the larger group.

1. What types of organizations would benefit from implementing an anti-bribery management system based on the ISO 37001 standard?
   - Why?
2. What are the factors that make them a good ISO 37001 candidate?
3. What additional benefits would they get from adopting the standard (*since they may already have legal anti-bribery obligations)?*

15 Minutes

Reflection – we have covered…

- ISO
- ISO 37001 creation
- Practical differences between FCPA and ISO 37001
- Benefits of ISO 37001 certification:
  - Operating
  - Strategic
- Other high level aspects of the standard

1. What is Bribery ?

2. What is the FCPA?

3. What is ISO 37001?

4. How does ISO 37001 work?

5. How do I prepare for an ISO 37001 audit?

Together we will cover…

How ISO 37001 operates, to include:

- ISO's *High Level Structure*
- ISO 37001 requirements and definitions
- Risk assessment and operational priorities
- Roles and responsibilities
- Managing and improving the system

A Polling Question

How many of the organizations in today's session have already been certified under another ISO standard, such as… ?

- ISO 9001 Quality Management Systems
- ISO 14001 Environmental Management Systems
- ISO 27001 Information Security Management Systems

High Level Structure (HLS)

All ISO management system standards created or revised after 2012 use a common framework containing:

- Unified High Level Structure
- Common Text and Terminology

Individual management systems standard add additional "discipline-specific" requirements as required

Significance?

- Organizations that are ISO 9001, 14001 or 27001 – certified (or aligned) are already familiar with ISO 37001 HLS structure and approach
  - ISO 37001 adoption will require less time and resources

Annex SL/HLS - Core set of requirements!

1. Scope
2. Normative reference
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operations
9. Performance evaluation
10. Improvement

ISO 9001 additions

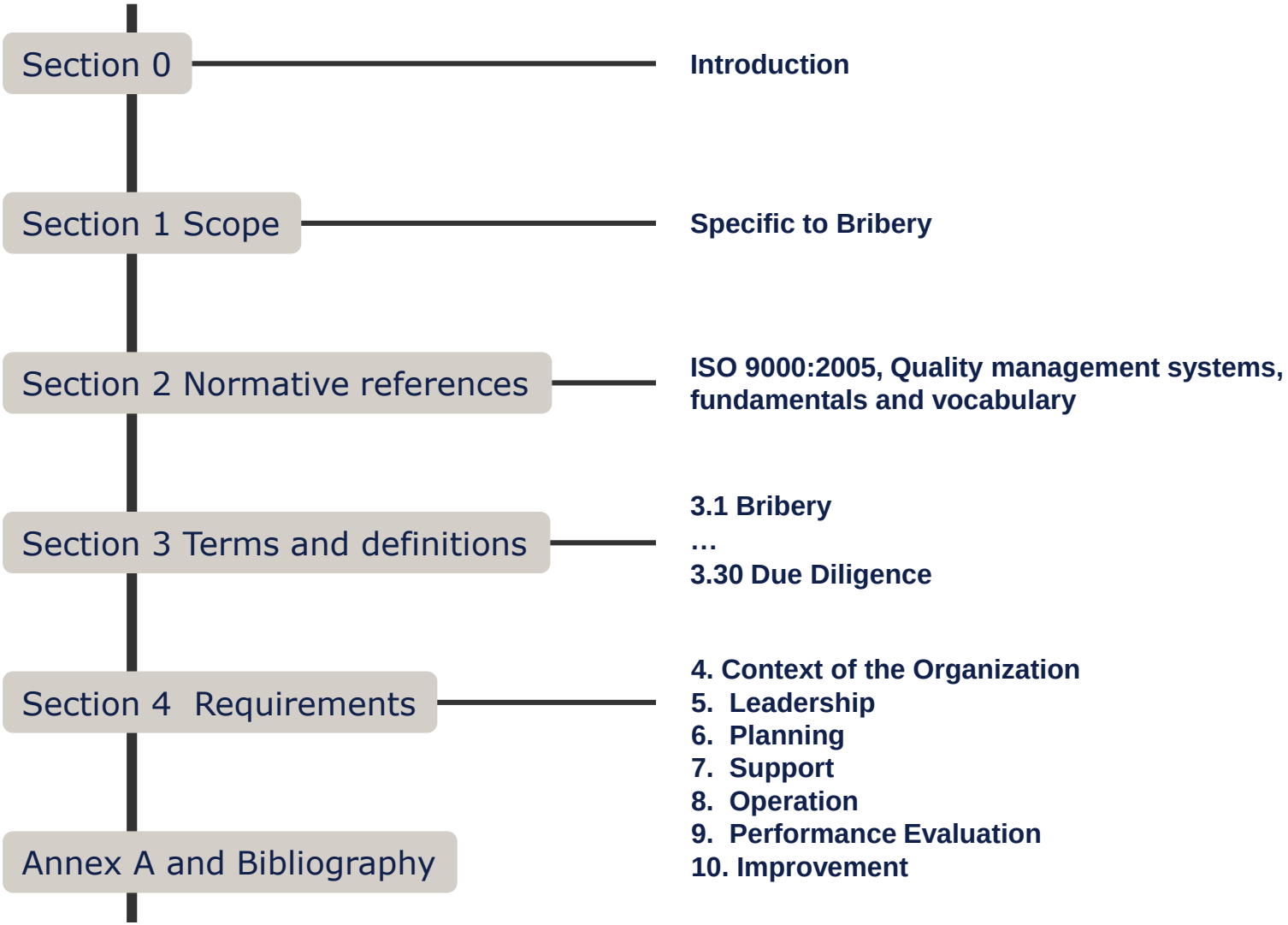
ISO 14001 additions

ISO 27001 additions

ISO 37001 additions

Individual management systems standard add additional "discipline-specific" requirements as required

ISO 37001 standard at a glance



Scope of ISO 37001 standard

Bribery (generally):

Section 3.1 – "offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial) directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties." (emphasis added)

- **Note 1** – "The above is a generic definition. The meaning of the term "bribery" is as defined by the applicable anti-bribery law applicable to the organization and by the anti-bribery management system designed by the organization."
- **Significance:**
  - "The law is the law"
  - Flexibility
    - Opportunities to go "above and beyond"

What does ISO 37001 not cover? (ref: ISO37001:2016)

- ISO 37001 does not specifically cover corrupt practices such as:
  - Fraud
  - Cartels and other anti-trust/competition offenses
  - Money-laundering
  - Cybercrime

But…

- These crimes and corrupt practices often involve bribery
- Adopting ISO 37001 may help reduce the risk of these other practices from occurring

Impact 4: Getting to know the standard

Review of ISO 37001 requirements

- Follow along in your copy of ISO 37001
- As we review each requirement together, consider the following:
  - How does our organization meet the standard requirements?
  - What evidence (if any) is required to ensure adequate implementation?
- Highlight your copy of the standard using the following conventions:
  - Requirements (shalls) = Yellow
  - Monitoring activity = Green
  - Documented information = Blue

Impact 5: Bribery is a two (or more) way street

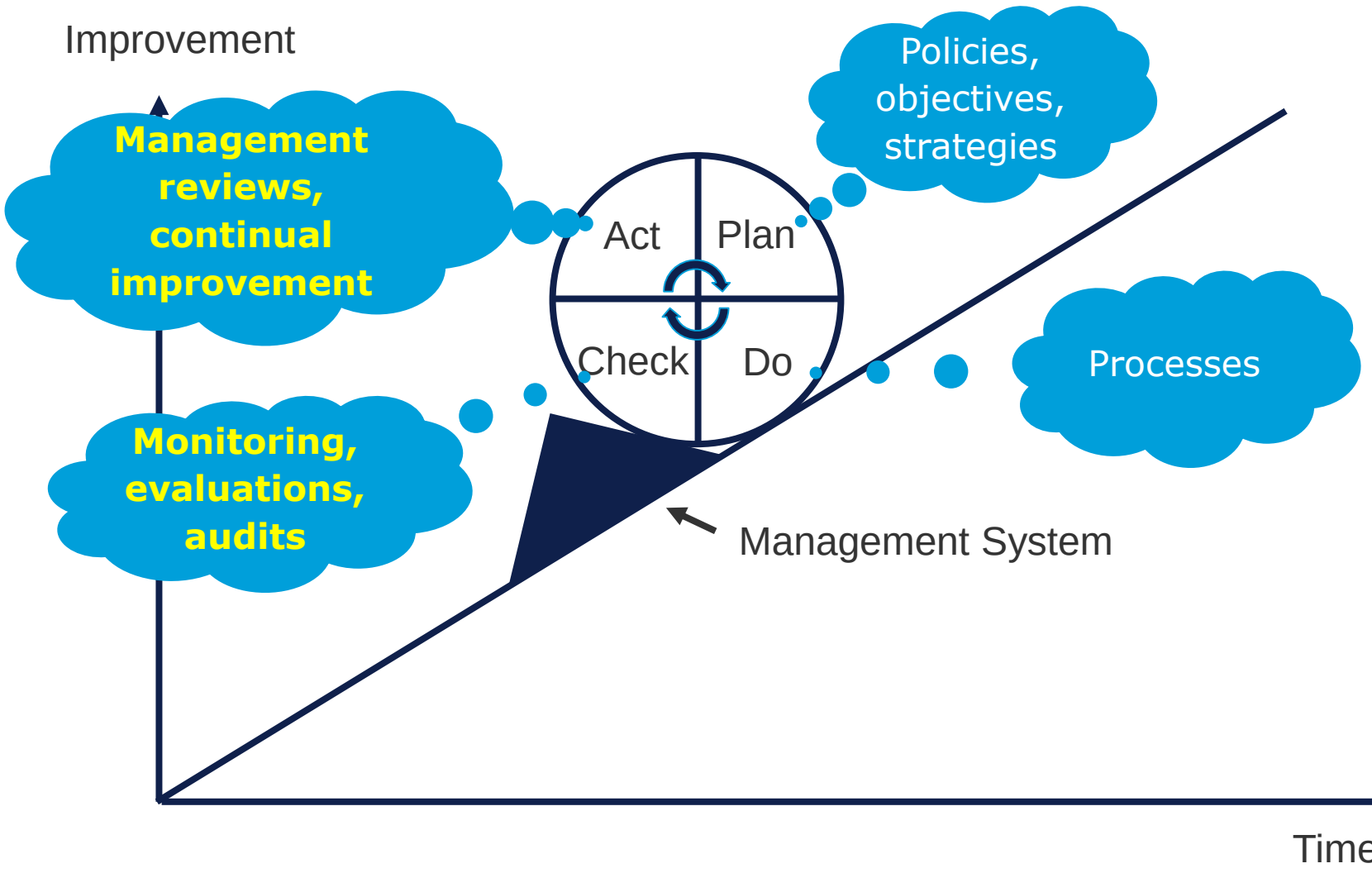
What does the following statement mean to your organization?

> "The measures necessary to prevent, detect and mitigate the risk of bribery *by the organization* can be different from the measures used to prevent, detect and respond to bribery *of the organization* (or its personnel or business associates acting on the organization's behalf)"

- Refer to ISO 37001, Annex A.8.4.
- Keep track of your ideas and be prepared to present to the larger group.

10 minutes

Cycle: Plan ● Do ● Check ● Act



DNV·GL

Impact 6: Requirements

- Focus on sections:
  - 4 Context of the Organization
  - 5 Leadership
  - 6 Planning
- Work in groups, review all materials (levels and sublevels) in the sections, and discuss and list the following:
  - 1. Documentation (and other) requirements
  - 2. Related processes

10 Minutes

Section 4.5 - Bribery Risk Assessment (BRA)

- Foundational
  - ISO 37001 management system and it's scope (4.3) is a function of the bribery risk that is identified, analyzed, managed, and measured/monitored through the BRA
- Tied to it are other foundational sections – the understanding of:
  - 4.1 Organization and its context
  - 4.2 Stakeholders' needs and expectations
- Scope of ABMS likely to change, as business changes
  - New markets, products/services – organically or through mergers/acquisitions
  - Sector developments – e.g. oil and gas FCPA enforcement

Common Bribery-related Risk Factors

Generally – apply the investigatory point of view and consider

- Who?
- What?
- Where?
- Why?
- When?

Organizational structure

- HQ/field offices/branches
- Joint ventures
- Partnerships

Organizational activities

- Sales
- Marketing
- Procurement
- Bidding

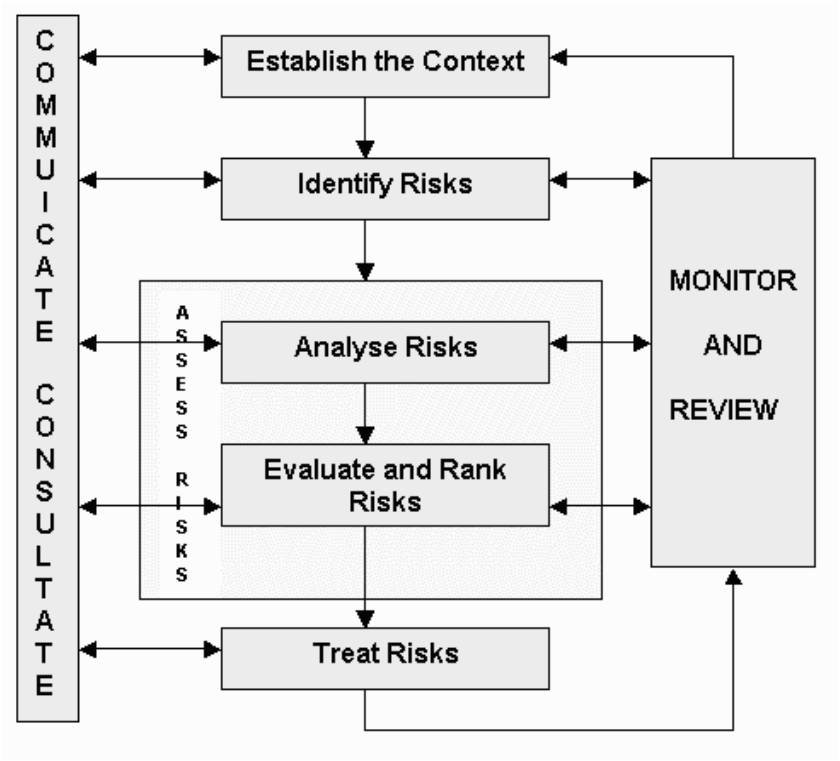
Organizational books/records – historically problematic areas

- Gifts
- Entertainment
- Charitable contributions
- Political donations
- Cash and related accounts
- Accounts payable

Legal requirements

- FCPA – US companies, business conducted in US, with US nationals or involving US banks
- UKBA?
- Other applicable law?

'Risk-based Thinking' Models – *Ways to think about risk!*



PDCA Approach

DNV·GL

Risk-based Thinking as a Part of the Management System

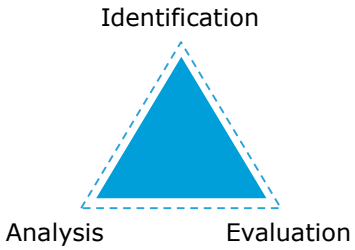
First determine the:

4.1 Internal & external business context

4.2 Expectations of interested parties

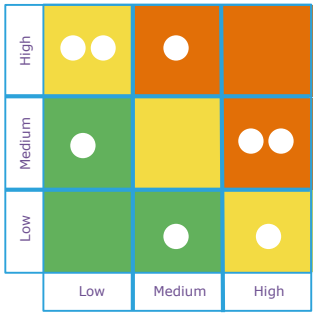
Then conduct:

4.5 RISK ASSESSMENT

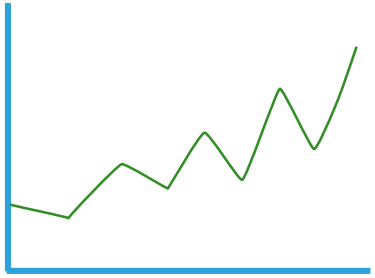


Resulting in:

IMPACT REPORT

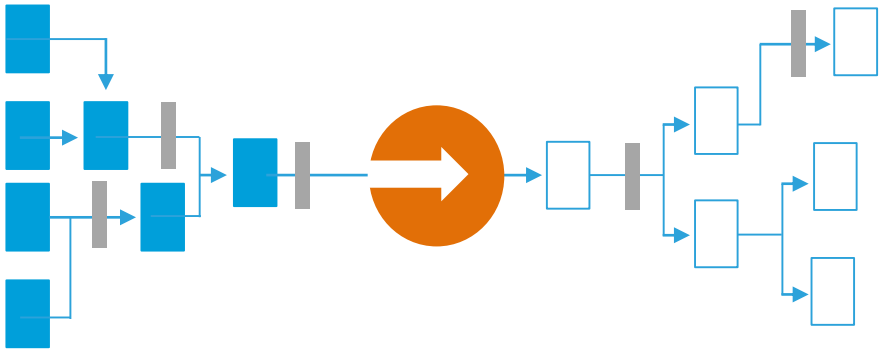


Measure / evaluate effectiveness



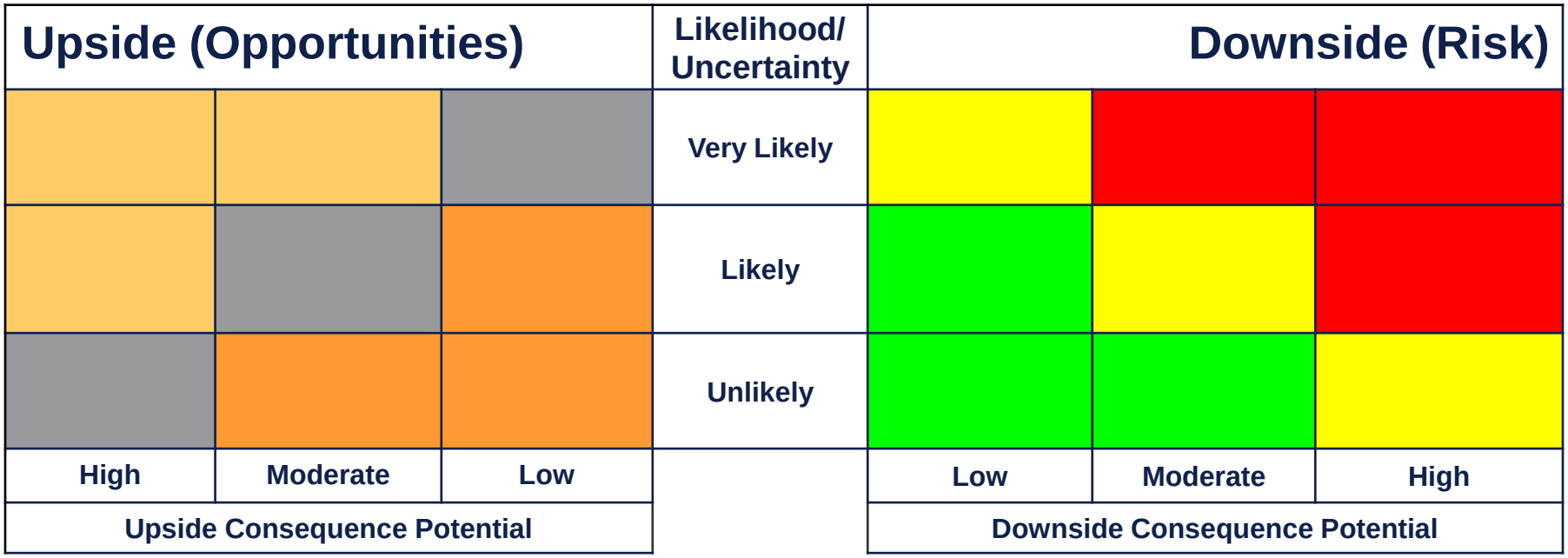
Embed relevant actions and controls into management system processes

CONTINUOUS IMPROVEMENT



DNV·GL

Qualitative Analysis: *Risk Matrix as a Reporting Tool for Risk Assessment*



Risk Rating	
Gold	Green
Silver	Yellow
Bronze	Red

DNV·GL

Leadership (5) and Planning (6) Required

- Generally, ISO 37001, as compared with legal standards, is ***more specific*** and direct on what to do and how to do it – to help identify and prevent bribery
  - Also, and seemingly not understood or appreciated by many legal commentators, these ABMS (business standard) requirements support and strengthen (and are not intended to replace or substitute for) the legal standards!
- **Leadership** - "demonstrate leadership and commitment with respect to ABMS by…"
  - 5.1.1 d) [Board] "requiring that adequate and appropriate resources needed for the effective operation of the [ABMS] are allocated and assigned"
  - 5.1.2 b) [Management] "ensuring the integration of the [ABMS] into the organization's processes"
    - just one of fourteen specific management directives

Leadership (5) and Planning (6) Required

- Leadership (cont.)
  - 5.3.3 [Management] For delegated processes where there is more than a low risk of bribery, organization must establish and maintain processes and controls that safeguard against actual or potential conflicts of interest, *and* management must ensure that processes/controls are reviewed periodically as part of its role and responsibility for ABMS implementation and operation.
- *Point*: not just "oversee" or "direct" or "take actions consistent with the policy…"
- Instead, because of the historical nature and severity of the conflict of interest risk:
  - Risk identification
  - Risk management through requirements:
    - Processes/controls
    - Review
    - Responsibility

Leadership (5) and Planning (6) Required

- Planning
  - 6.2 The organization shall establish [ABMS] objectives at relevant functions and levels. The [ABMS] objectives shall:
    - a) be consistent with the anti-bribery policy
    - b) be measurable (if practical)
    - c) take into account applicable factors referred to in 4.1 [context], the requirements referred to in 4.2 [stakeholders] and the bribery risks identified in 4.5 [bribery risk assessment]
    - d) be achievable
    - e) be monitored
    - f) be communicated in accordance with 7.4 [communication]
    - g) be updated as appropriate
    - Other language concerning who, what , how and when…
- *Point*: Specific obligations/conditions – ***with*** **documentation requirement**

Roles/Responsibilities: Senior Levels

Board (Governing body): *Oversight*

- 5.1.1 (as noted above) "ensuring that the organization's strategy and anti-bribery policy are aligned….receiving and reviewing information about the ABMS…requiring that adequate and appropriate resources needed for effective operation of the ABMS are allocated and assigned…."
- 9.3.2 "undertake periodic reviews of the [ABMS] based on information provided by top management and the anti-bribery compliance function and any other information that the governing body requests or obtains"
- 7.2.2.2 c) Periodic policy compliance declaration procedure requirement

Management (Top management): *Operational*

- 5.1.2 b) (as noted above) "ensuring the integration of the [ABMS] into the organization's processes"
- 5.1.2 a) "ensuring that the [ABMS], including policy and objectives, is established, implemented, maintained and reviewed to adequately address the organization's anti-bribery risks"
  - Laundry list of other requirements e.g. promoting: an anti-bribery culture – h) and continual improvement i)

Roles/Responsibilities: Employees

- 5.3.1 The governing body (if any), top management and *all other personnel shall be responsible for* understanding, complying with and applying the anti-bribery management system requirements, *as they relate to their role in the organization.*
- 7.3 Awareness & Training - Personnel shall be provided with anti-bribery awareness and training on a regular basis (at planned intervals determined by the organization), as appropriate to their roles, the risks of bribery to which they are exposed, and any changing circumstances. *The awareness and training… shall be periodically updated as necessary to reflect relevant new information.*

Roles/Responsibilities: Compliance Function (5.3.2)

- Management requirement to *"assign the responsibility and authority"* to anti-bribery compliance function for [ABMS]:
  - Design and implementation
  - Advice and guidance
  - Conformance to ISO 37001 requirements
  - System performance reporting to Board and Management
  - Also: Function shall have *"direct and prompt access"* to Board and Management concerning *"any issue or concern"* relating to bribery or ABMS

ISO 37001 recognizes that the compliance function needs: (a) adequate resources; and (b) appropriate competence, status, authority and independence

What is Due Diligence?

Due Diligence

Process to further assess the nature and extent of the bribery risk and help organizations make decisions in relation to specific transactions, projects, activities, business associates and personnel.

ISO 37001:2016, 3.30

Roles/Responsibilities: Human Resources (7.2.2.2)

For positions with more than a low bribery risk, organization **shall implement procedures** covering:

- a) **personnel due diligence**:
  - before they are employed
  - before they are transferred or promoted
  - to determine "as far as is reasonable" that:
    - it is appropriate to employ or redeploy them; and
    - they will comply with the ABMS and ISO 37001 requirements
- b) **incentive compensation** reviewed periodically to verify that there are reasonable safeguards in place to prevent compensation from encouraging bribery [POLICY]
- c) **compliance declarations** filed periodically by more than low bribery risk personnel, management, and the board, confirming their compliance with the organization's anti-bribery policy [POLICY]

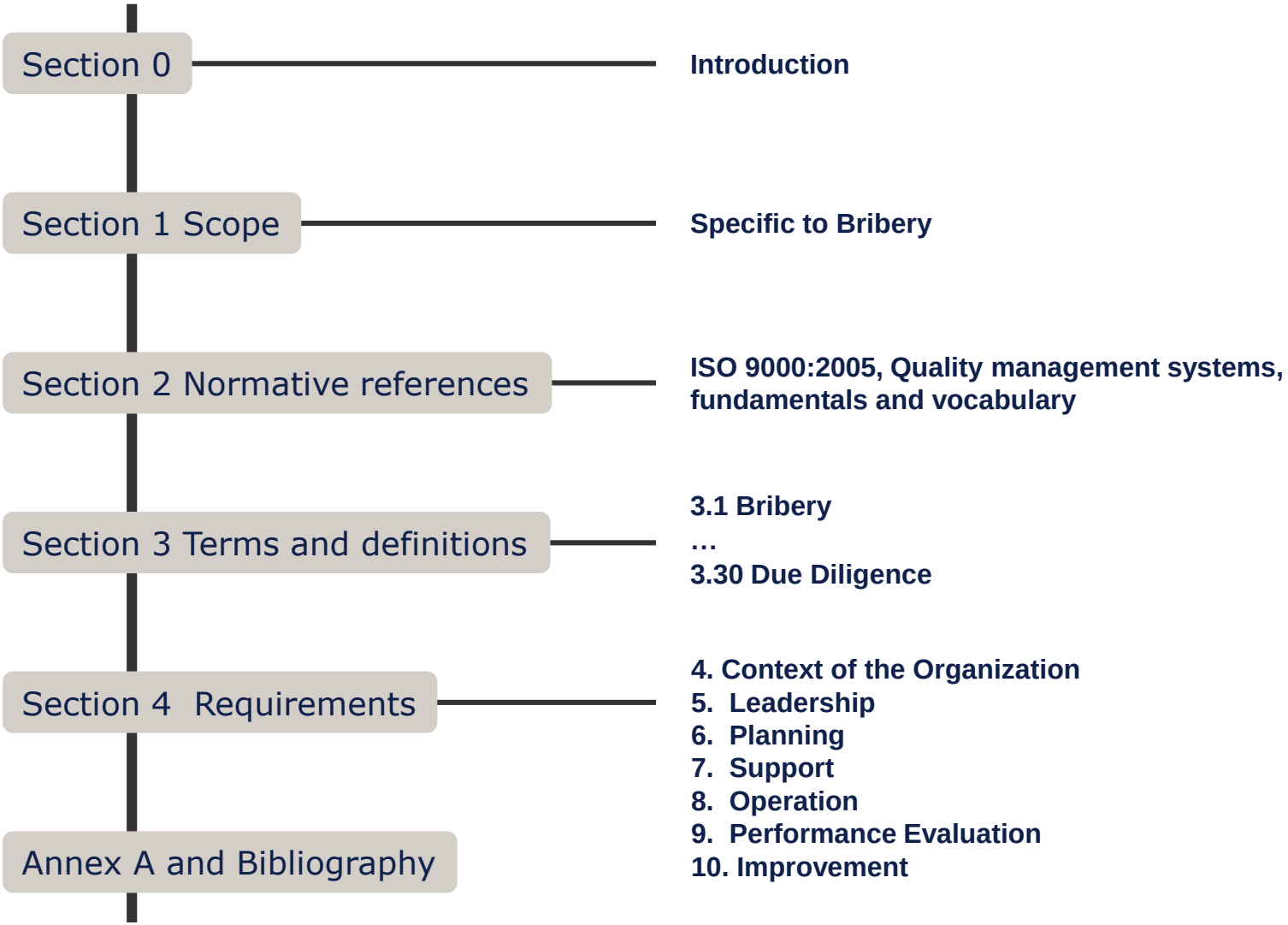
Impact 7: Competence Specific to Anti-bribery

Discuss Section 7 and these questions (and be prepared to present):

- What are the various requirements on competence management in Section 7.2, including:
  - Actions
  - Procedures
  - Documentation
- What are the anti-bribery priorities and themes underlying these sections?

10 Minutes

ISO 37001 Standard at a Glance (revisited)



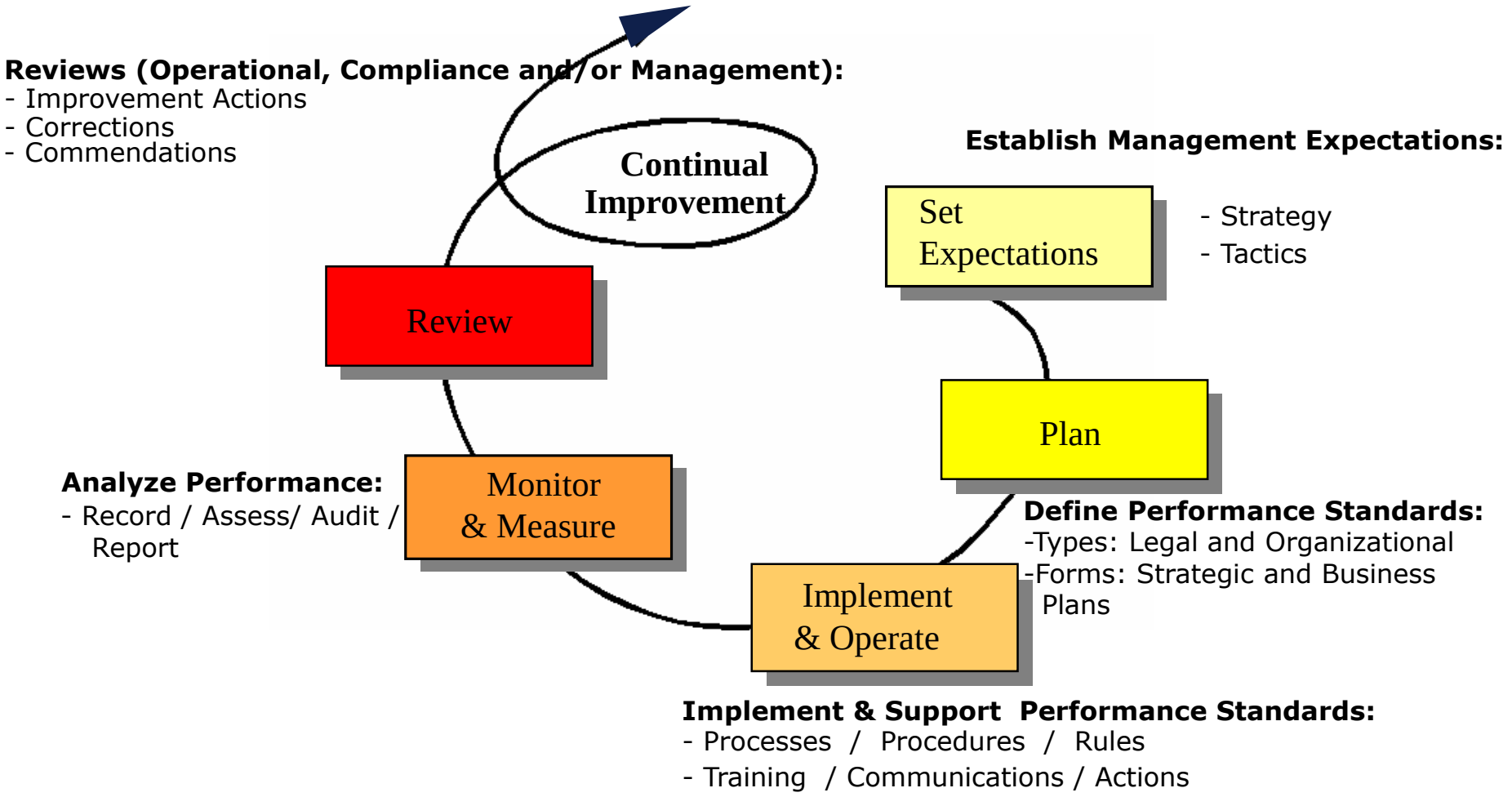
Operations (8) – Overview and Observations

- Some parts are substantive, and specific
  - Other parts are general, and broad – e.g. 8.3 Financial Controls - and 8.4 Non-Financial controls – referencing Appendices with more detailed treatment
- **Important**: 8.1 Operational planning and control – "keep.. documented information to the extent necessary to have confidence that the processes have been carried out as planned…"
- FCPA "hot buttons":
  - Due diligence – 8.2
  - Gifts, hospitality, donations – 8.7
  - Reporting procedures/raising concerns (with anonymity) – 8.9
- Putting anti-bribery commitment into action:
  - Externally - anti-bribery control implementation by others: controlled organizations and business associates
  - Internally - managing inadequacy of anti-bribery controls

Performance Evaluation (9) – Overview and Observations

- As with other management systems, an emphasis on *monitoring, measurement, analysis and evaluation (9.1)*
  - Importance highlighted by documentation retention requirement:
    - After detailed "what, who, methods detail, when, and to whom reported…"
    - Retain "appropriate documented information as evidence of the methods and results"
- *Internal audit* plays a key system testing role (9.2), auditing conformance with:
  - Organization's own ABMS requirements; and
  - ISO 37001 requirements; with a
  - Documentation requirement: "evidence of the implementation of the audit program and the audit results" 9.2.2 e)
- *Board review (9.3.2)* and *management review (9.3.1)* also involve documentation retention requirements concerning review results.

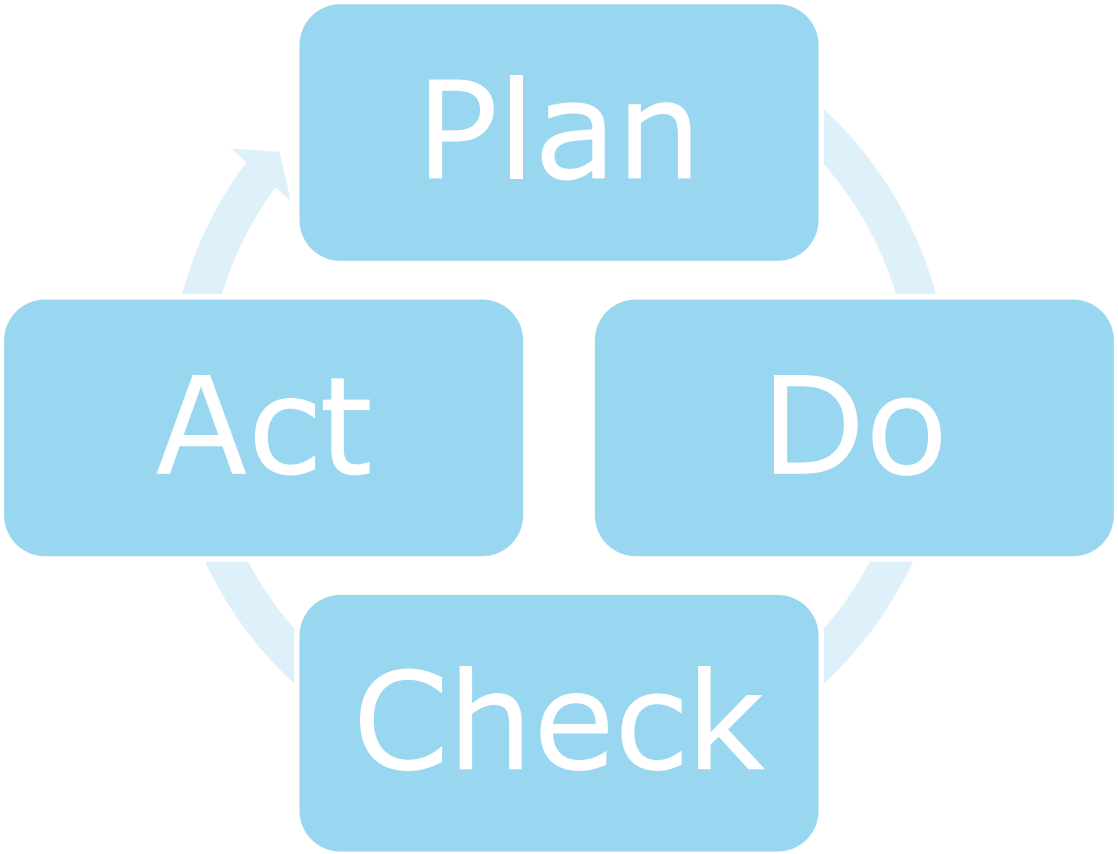
Risk Management and Performance Management



Improvement (10) – Overview and Observations

- As with other management systems, an emphasis on *Improvement (10)*
  - Importance highlighted by documentation retention requirement:
    - In addition to other requirements that are necessary once a nonconformity occurs, the organization must retain documentation to show "the nature of the nonconformities and any subsequent actions taken" and "the results of any corrective action" (10.1)
- *Continual improvement (10.2)* importance –
  - Suitability, adequacy and effectiveness of the ABMS

Continual Improvement is a Mindset



Summary and Themes of Sections 4 - 10

- ISO 37001 management system not the same as a FCPA program
- Bribery risk assessment (BRA) is foundational – to determine ABMS scope
- Specific (and relatively expansive) roles and responsibilities
- ISO 37001 involves basic management tasks (e.g. numerous explicit requirements and associated documentation)
- Active, dynamic approach: PDCA methodology - Plan, Do, Check, Act

Reflection – we have covered…

How ISO 37001 operates, to include:

- ISO's *High Level Structure*
- ISO 37001 requirements and definitions
- Risk assessment and operational priorities
- Roles and responsibilities
- Managing and improving the system

1. What is Bribery ?

2. What is the FCPA?

3. What is ISO 37001?

4. How does ISO 37001 work?

5. How do I prepare for an ISO 37001 audit?

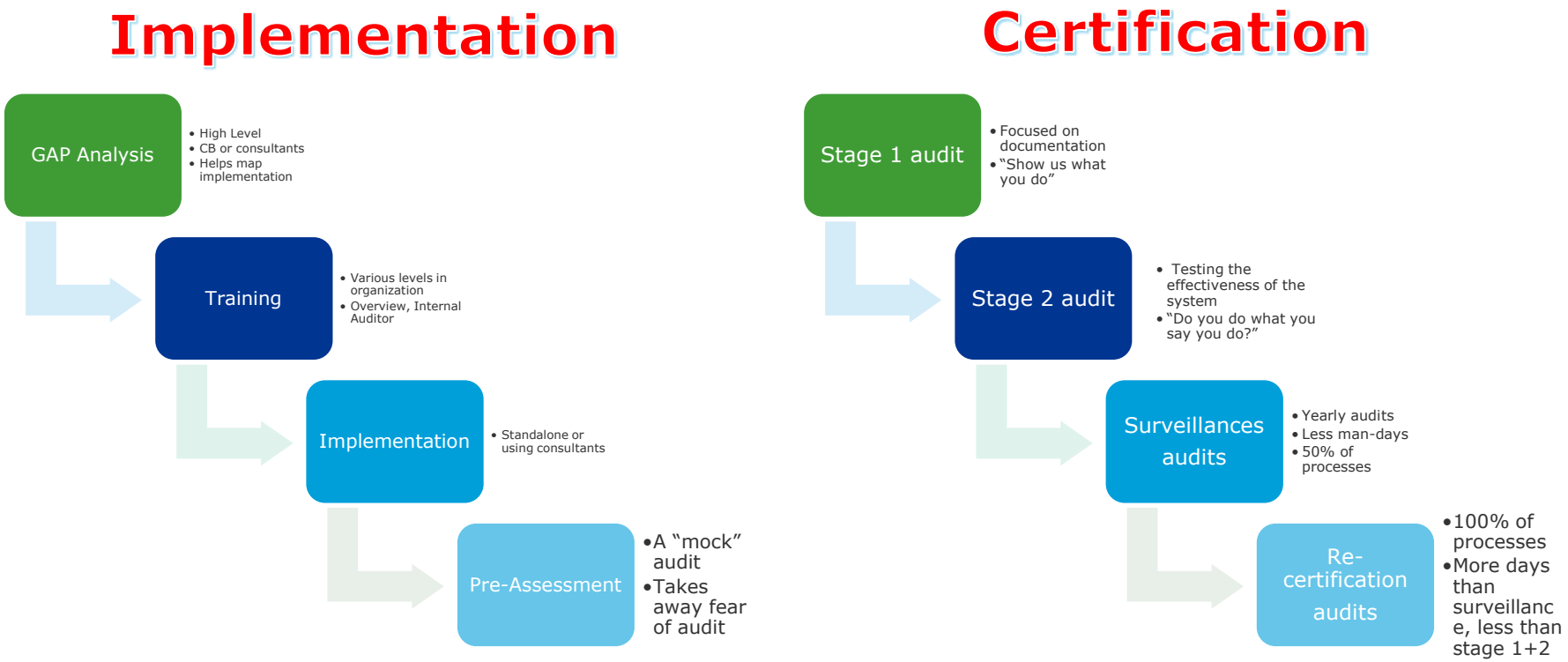
Together we will cover…

- External value propositions
- Preparing for a certification audit
- Next steps

Certification Value and Process

- Certification = External Value Proposition
  - Organization is a better partner/supplier/investment etc.
  - Less risk: taken affirmative steps to manage a high risk area
  - An independent accredited 3rd party (certifying body [CB]) has conducted a rigorous audit that tests both design adequacy and operating effectiveness and has determined that the organization's anti-bribery management system complies with the requirements of ISO 37001
  - What does "getting certified" mean?
  - Two stage initial review:
    - Stage I: Documentation review
    - Stage II: System review
  - Three year certification duration – based on periodic additional reviews
    - Initial
    - Anniversaries (1st and 2nd) - with substantially reduced scope

The Certification Process



On What Basis is the Certification Provided by the Certifying Body?

Reasonable Assurance

- Based on review, testing and sampling
- Same standard as is applied to audit of a public company's financial statements by its CPA firm
  - e.g. Marriott International 2017 Form 10-K
- REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

  "…We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud…"
- Not a guarantee
- Not based on exhaustive (and costly) deep dive (e.g. forensic investigative review)
- Review cycle (management and audit) needs to have occurred

Preparing for the Certification Audit

- Leverage existing organizational standards recognition
- Business: ISO 9001, 14001, 20000, 27001
- Legal FCPA and/or other applicable anti-bribery law
  - Perform gap assessment: ISO 37001 vs. legal standard(s)
  - Good news: with a good FCPA program in place, the majority of an ISO 37001 management system is in place
- Generally - document, document, document
- Specifically, as recommended "readiness" activities, focus on:
  - BRA
    - Integral to the scope of the ABMS
  - Requirements
    - Hard and, as applicable, soft varieties
  - PDCA
  - Management system certification, not a program certification

Next Steps – General Recommendations

***Communication*: Begin the internal discussions**

- With organizational leadership: getting value (e.g. increasing confidence in government, supporting rule of law) through certification from anti-bribery/anti-corruption activities and costs
- With GC (for commercial entities): supporting organization's anti-bribery /anti-corruption compliance **program** with ISO 37001 **management systems** processes
- With Governing body: strategic and oversight benefits
- Get additional standard-related information
- See **www.iso37001info.org**

***Operationalization*: Focus on operations and the related higher-bribery risk areas**

Documentation*: Policies, processes, protocols – coverage *and*, as appropriate, monitoring, measurement, analysis all working towards *continuous improvement

Impact 8: Participant ISO 37001 Take-Aways

Answer these questions:

- ”Elevator Speech” preparation: If my boss asked me - What is the primary benefit of ISO 37001 certification? – how would I respond?
- What will be needed (internally) to successfully implement the standard?
- What are my next steps?
- What are my take-ways that I want to remember or further research after this course?

Final Thoughts – Why ISO 37001?

ISO 37001 adoption allows governmental organizations to…

- Demonstrate leadership and concern for citizens
- Project power to outside world
- Support economic growth

Acceptance/interest is growing

- Governments are applying ISO 37001
- Development banks/aid agencies are also reviewing the standard
  - Show prudent sustainability activities to stakeholders
- Law enforcement – the standard is getting recognition and validation in case settlements:
  - Odebrecht (Brazil) – will obtain ISO 37001 certification
  - Area Denmark (Denmark) – has obtained ISO 37001 certification

Reflection – we have covered…

- External value propositions
- Preparing for a certification audit
- Next steps
- Participant take-aways
- Questions?
- Let’s continue the discussion!

Merci – thank you

Questions?

Worth MacMurray

worthmacm@gmail.com/ **+1 703-300-6345**

Bruno Samuel

bruno.samuel@dnvgl.com/ **+1 832-418-4799**

www.dnvgl.com

SAFER, SMARTER, GREENER