



Risk Management to Contingency Planning

ICD-10 Operational Readiness

Keith Hatch, Florida Blue (BCBS of Florida), Senior Manager

Agenda



- Definitions
- Relationship between risk management, contingency planning and operational readiness
- Let us talk “risk management”
- The risk management and contingency planning process structure
- Obtaining operational readiness
- Benefits
- Appendices

DEFINITIONS

Risk Management

What is it?

- Risk is ...
 - possibility of an event;
 - impacting the achievement of objectives; and,
 - measured in terms of impact and likelihood.”
- Risk appetite is ... level of risk that is acceptable by the organization.
- Risk Management is ... “A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objective.” ¹

¹ <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards-Glossary.aspx>

Contingency Plan

What is it?

- A ***process and documentation to remediate identified business impact events to ensure the entities existence and profitability***, as an on-going concern.
 - Operational efficiency and effectiveness
 - Reporting accuracy, completeness, and timeliness
 - Compliance (industry, associations, and governmental)
 - Strategic alignment (industry, associations, etc...)
- Remediation may take one of three forms:
 - Resolution (root cause/internal solutions)
 - Acceptance (both risk and impacts)
 - Transference of risk (legally through contractual agreements)

Operational Readiness

Defined as:

- As defined by US Code, operational readiness is
“the capability of an organization, an asset, a system, or equipment to perform the missions or functions for which it is organized or designed.”
(6 USC § 741)
- ICD-10 Operational readiness could be defined as:
 - The ability to receive, adjudicate and deliver an ICD-10 enabled transaction.
 - Without impacting the existing business processes.

**WHAT IS THE RELATIONSHIP BETWEEN RISK
MANAGEMENT, CONTINGENCY PLANNING AND
OPERATIONAL READINESS?**

Relationship



To maintain business continuity / operational readiness the relationship must be:

- Continuous
- Interdependent
- Complete
- Timely
- Cross-functional

Impacts of Inefficient and/or ineffective Risk Management



- Delayed contingency plans
- Inappropriate prioritization of issue remediation resources
- Negative publicity
- Potential compliance issues
- Inaccurate management decisions
- Unexpected business disruptions
- **MORE MONEY \$\$\$\$**

Impacts of Inefficient and/or ineffective Contingency Planning



- Inappropriate prioritization of issue remediation resources
- Negative publicity
- Potential compliance issues
- Inaccurate management decisions
- Operationally funded remediation (not capitalized)
- Unexpected business disruptions
- ***MORE MONEY \$\$\$\$***

LET US TALK “RISK MANAGEMENT”

COSO Risk Management Framework

Committee of Sponsoring Organizations (COSO) 2013 framework provides for:

- 3 objective categories :
 - operations,
 - reporting, and
 - compliance
- 5 components of managing risk:
 - controls (ie, policy)
 - risk assessment,
 - control activities (ie. trend analysis),
 - information and communication, and
 - monitoring activities.
- Provides adaptability to organization structure



Enterprise vs. Operational Risk Management



Differences

Enterprise Risk Management

- Top-down approach
- Corporate level risk (C-level)
- Focused on significant events
 - Strategy
 - Compliance
 - Legal
 - Public relations

Operational Risk Management

- Bottoms-up approach
- Functional level risk (Mgmt level)
- Focused on significant events
 - Process, system and resource
 - Reporting

Enterprise & Operational Risk Management

Using both provides:
greater opportunity to
identify risk events.

- Provides a complete corporate scope
 - Corporate
 - Operations
- Includes all risk categories :
 - Strategy
 - Compliance
 - Reporting
 - Operations

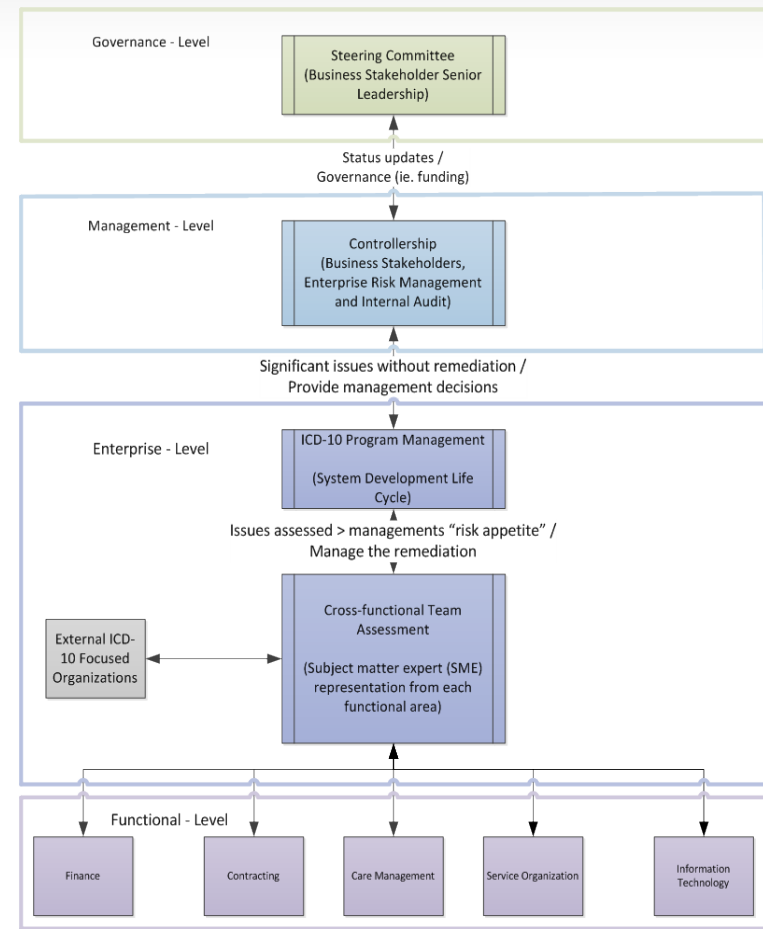


HOW DO YOU STRUCTURE THE RISK MANAGEMENT AND CONTINGENCY PLANNING PROCESS?

Risk Management / Contingency Planning Organization

General Structure

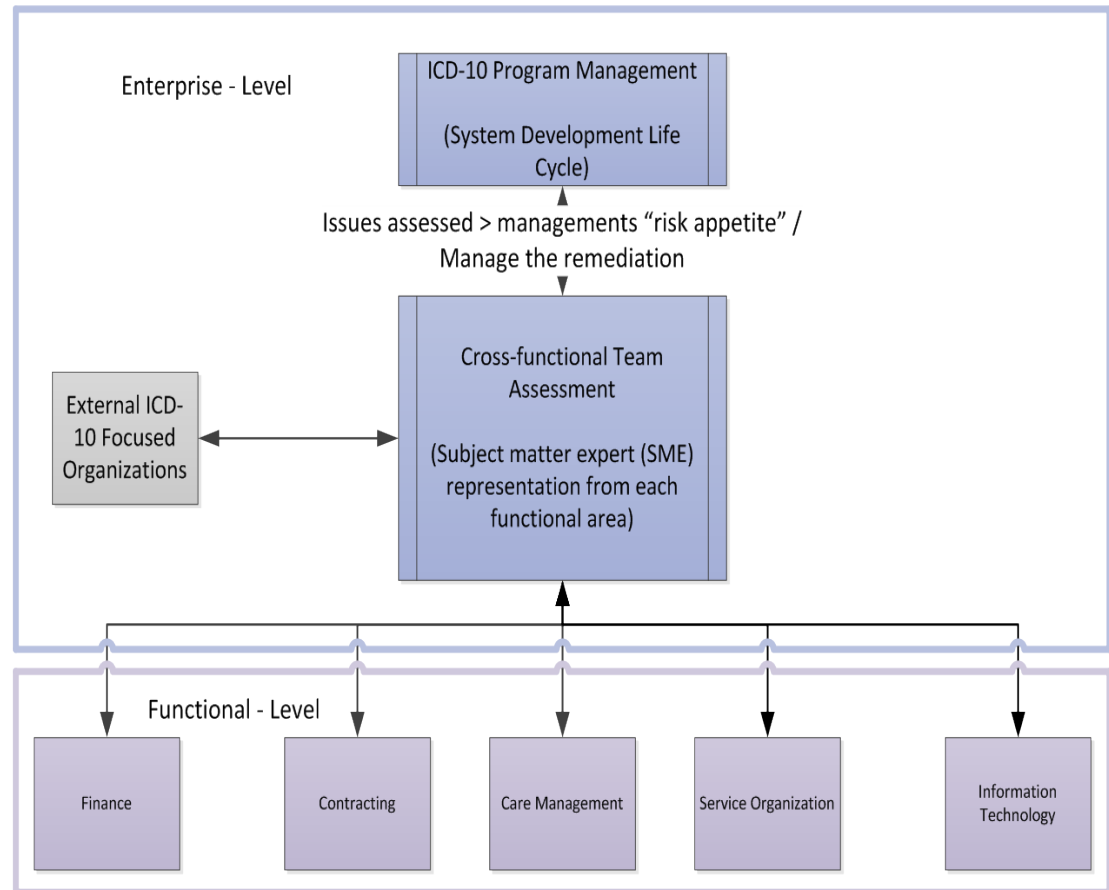
- Appends to or integrates and leverages the Program Structure.
- Organizational structure includes 4 levels
 - Program Organization
 - Governance
 - Program / Management
 - Function
 - Risk Management
 - Enterprise
 - Operational / functional



Risk Management / Contingency Planning Organization

Functional – Level

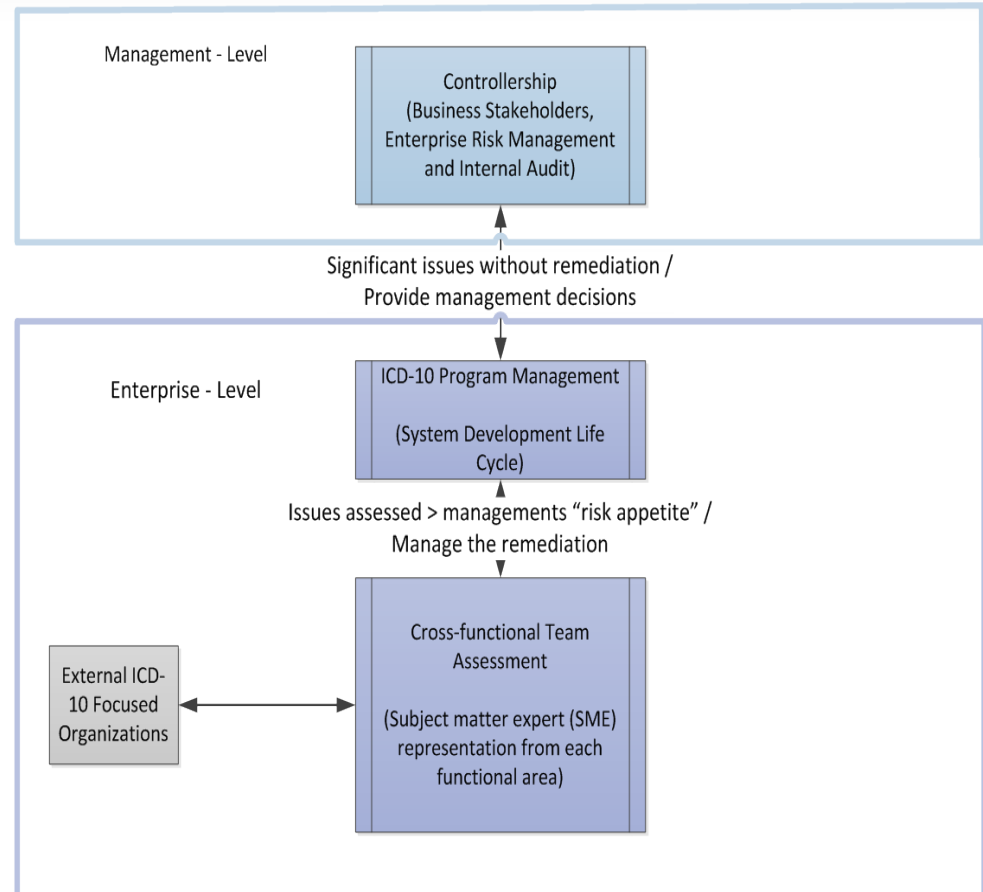
- Includes all relevant business areas
- Provides the **operational risk assessment** and the following functionality:
 - Functional testing
 - Issue identification
 - Business impact assessment (specific area impact)
 - Issue management and remediation
 - Issue reporting to / from Enterprise – Level



Risk Management / Contingency Planning Organization

Enterprise – Level

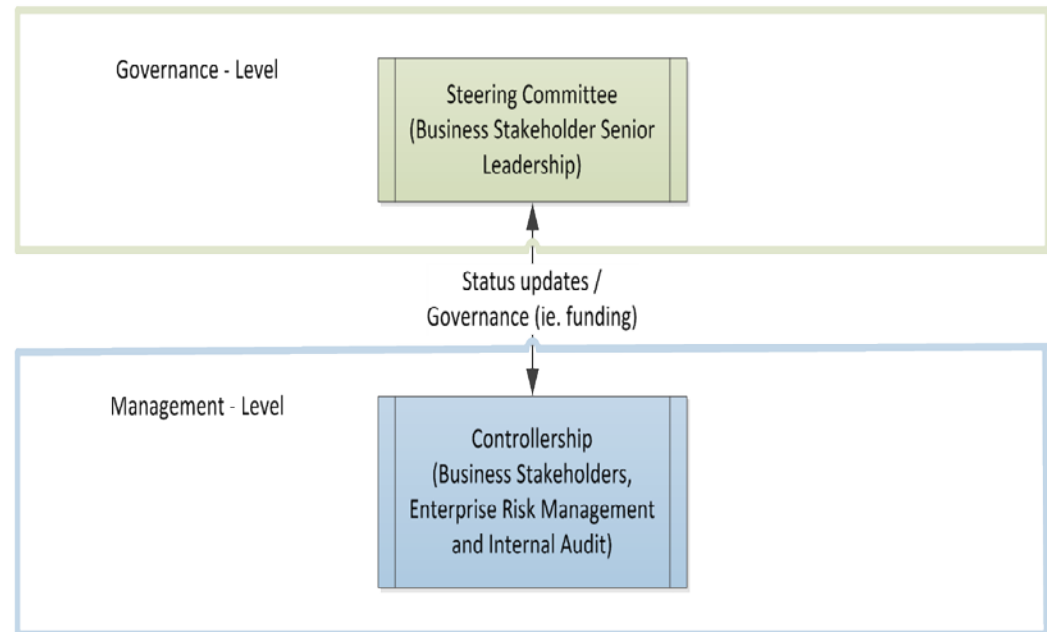
- Includes project/business leads and SMEs
- Provides a cross-functional **operational risk assessment**
- Identifies:
 - Transfer of risk
 - Existing remediation
 - External risks
- Validates the functional risk assessment
- Communicates significant risk to the Management – Level.



Risk Management / Contingency Planning Organization

Management – Level

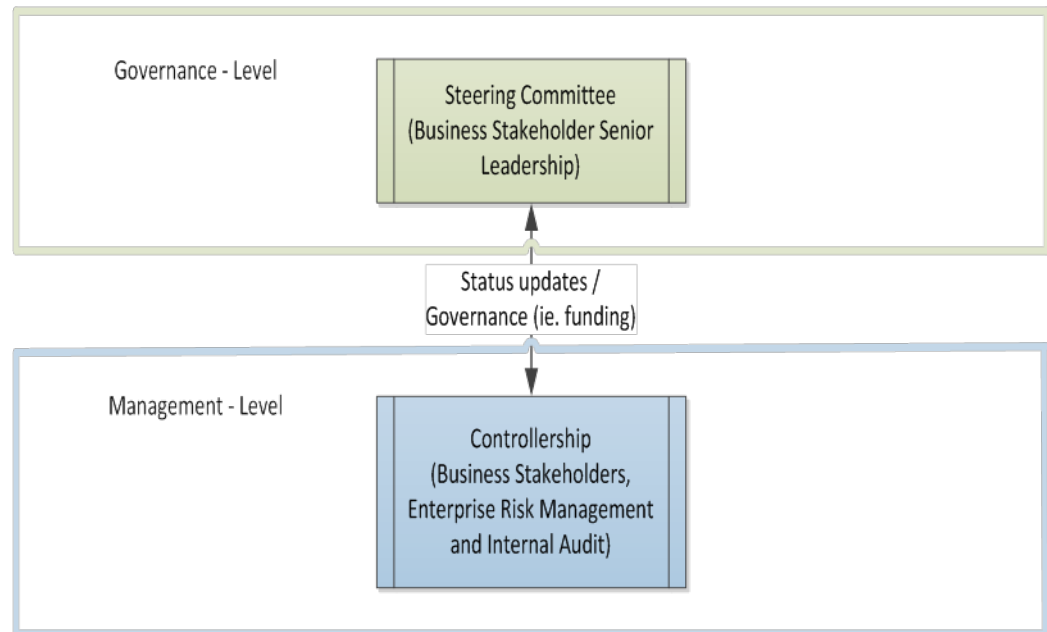
- Includes program leadership and business directors/leads
- Provides the **enterprise risk assessment**
- Identifies strategic and/or industry level risk/remediation.
- Provides functional direction and guidance
- Communicates project status and significant risk to the Governance–Level.



Risk Management / Contingency Planning Organization

Governance – Level

- Includes the Corporate champion (VP or higher), Senior Level management, and Program leadership
- Provides the **enterprise risk assessment**
- Provides general oversight, strategic direction and guidance
- Approves funding.



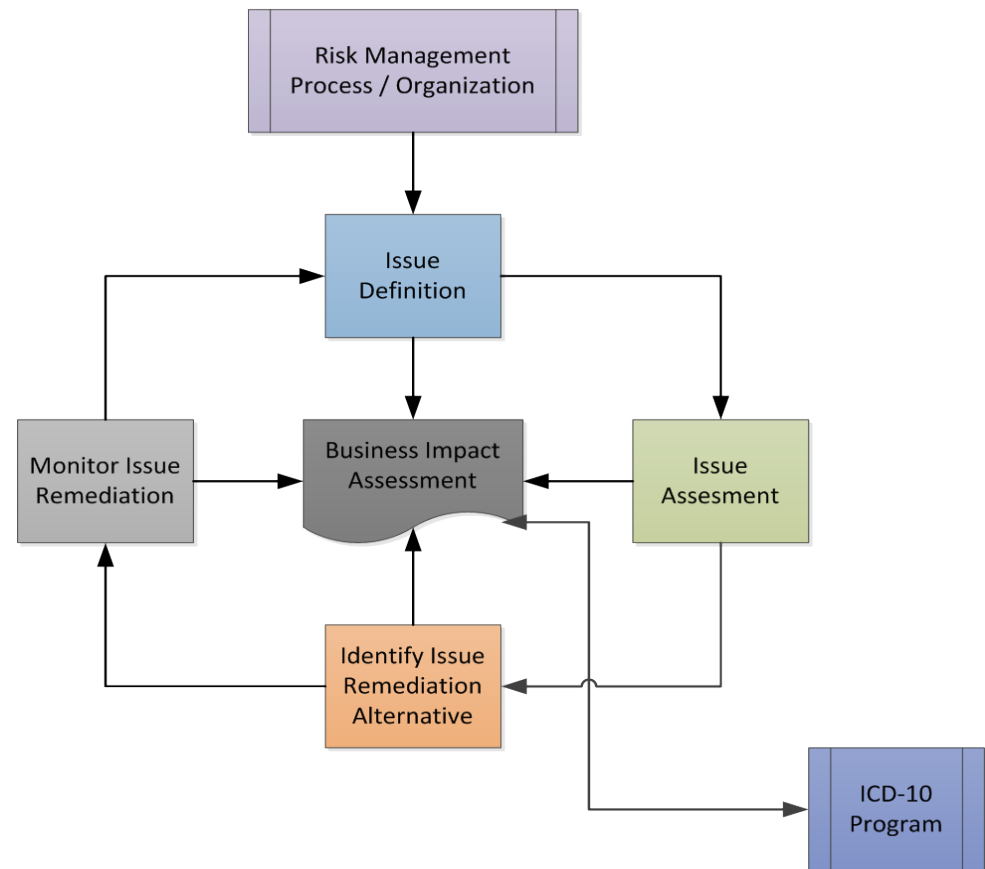
Operational Readiness

**USING RISK MANAGEMENT AND CONTINGENCY
PLANNING TO OBTAIN OPERATIONAL
READINESS?**

Operational Readiness

Business Impact Assessment Process

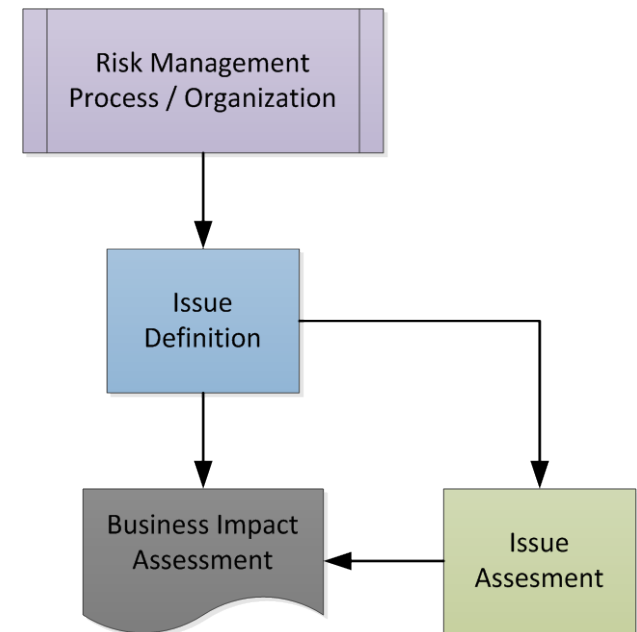
- Integrated into the:
 - Risk management process
 - Program System Development Life Cycle (SDLC)
- Includes full scope of enterprise knowledge
- Five (5) continuous parts following the issue identification:
 - Defining
 - Assessing
 - Remediating
 - Monitoring
 - Documenting



Operational Readiness

Issue Definition

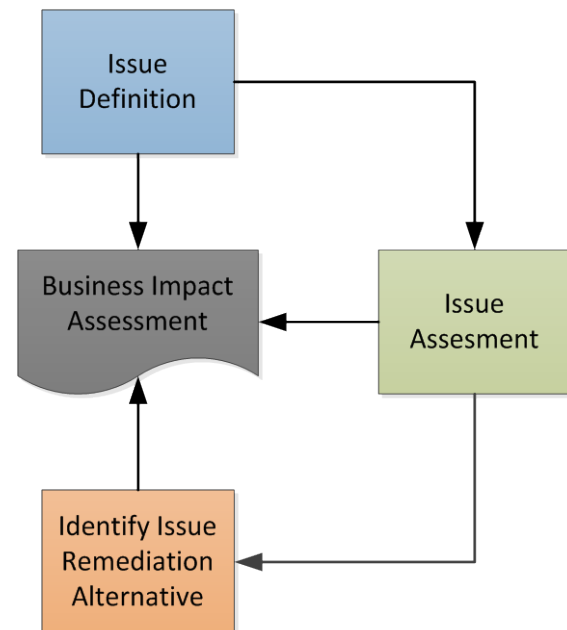
- Critical step of the assessment process
- Includes a clear concise issue statement that is:
 - Factual,
 - Quantifiable
 - Qualifying.
 - NOT vague and ambiguous.
- Answer some of these questions:
 - What is the impact event?
 - What or how does the event impact the business?
 - Who is impacted?
 - How often does it occur (time parameters)?
 - How does the event impact vary from the pre-defined operational metrics.
- Document



Operational Readiness

Issue Assessment

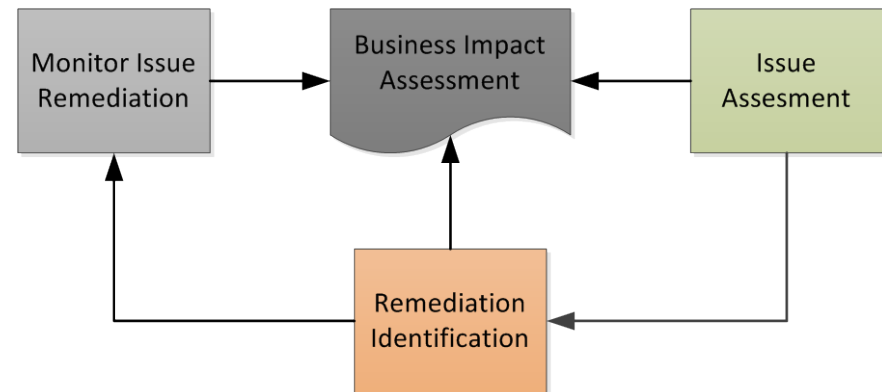
- A consistent metric to prioritize the issue.
- Uses the facts obtained in the issue definition process.
- Most business impact assessments include the following variables:
 - Impact
 - Frequency
 - Current remediation effectiveness (optional)
- Each assessed on a scale of 1-10
- Assessment rating = Impact X Frequency X CRE (Lowest impact = 1; and, Greatest = 1000)
- Document



Operational Readiness

Remediation Identification

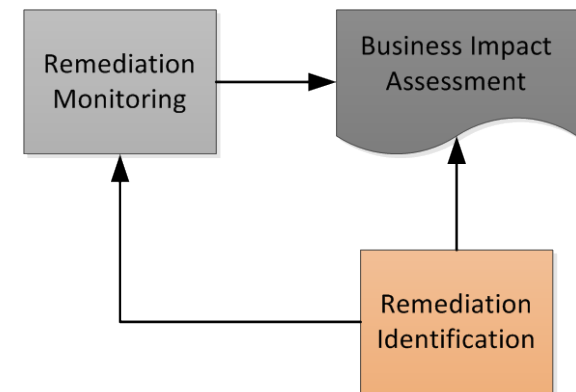
- Provides an opportunity to identify enterprise remediation alternatives
- Remediation can consist of:
 - Root cause remediation (system redesign, business rule configurations, business process redesign, etc...)
 - Acceptance / monitoring (within management's range of risk/business impact appetite)
 - Transference (legal or contractual conveyance of risk)
- Document



Operational Readiness

Remediation Monitoring

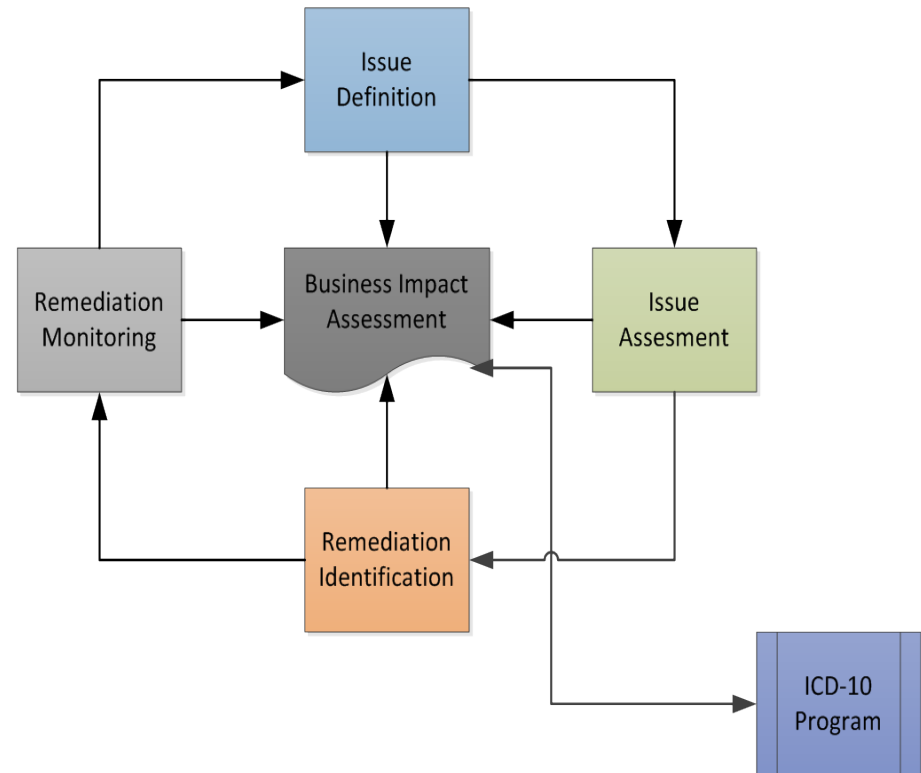
- Most often overlooked step in the process
- Biggest myth of risk management is “ONCE FIXED ALWAYS FIXED”
- Why is this a myth?
 - SYSTEMS - System logic is in a constant mode of flux during system development
 - TIME - Business changes with time
 - LEADERSHIP - Risk appetite changes with leadership and industry focus
- Periodically review remediated issues
- Document



Operational Readiness

Documentation

- Provides the business and IT Program a:
 - Point of reconciliation for the business and IT Program
 - Source of information to prioritize remediation efforts
- Critical for supporting:
 - Due diligence
 - Management decisions



Benefits



LIST OF BENEFITS FOR OPERATIONAL READINESS

Benefits



- Increased scope of issue identification
 - Internal (Enterprise and strategic)
 - External
- Holistic assessment of identified business impact / risk events.
- Added value of ICD-10 budgeted dollars through the prioritization of business impact remediation efforts and resources.
- Documentation to support due diligence
- OPERATIONAL READINESS

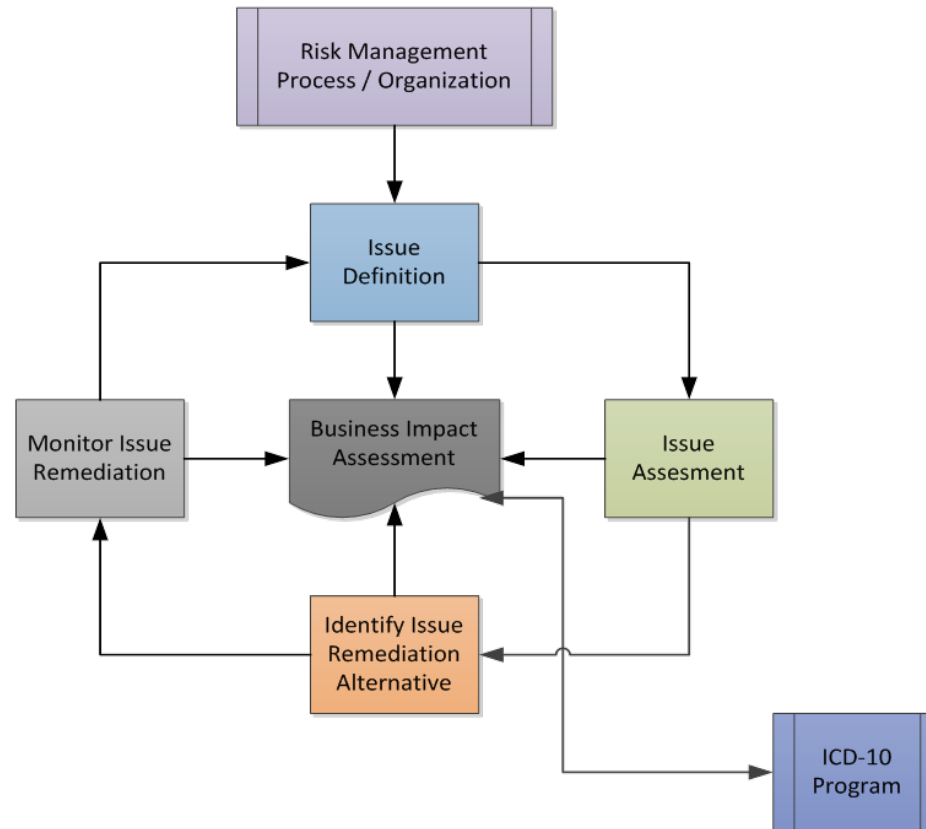
Operational Readiness



APPENDIX

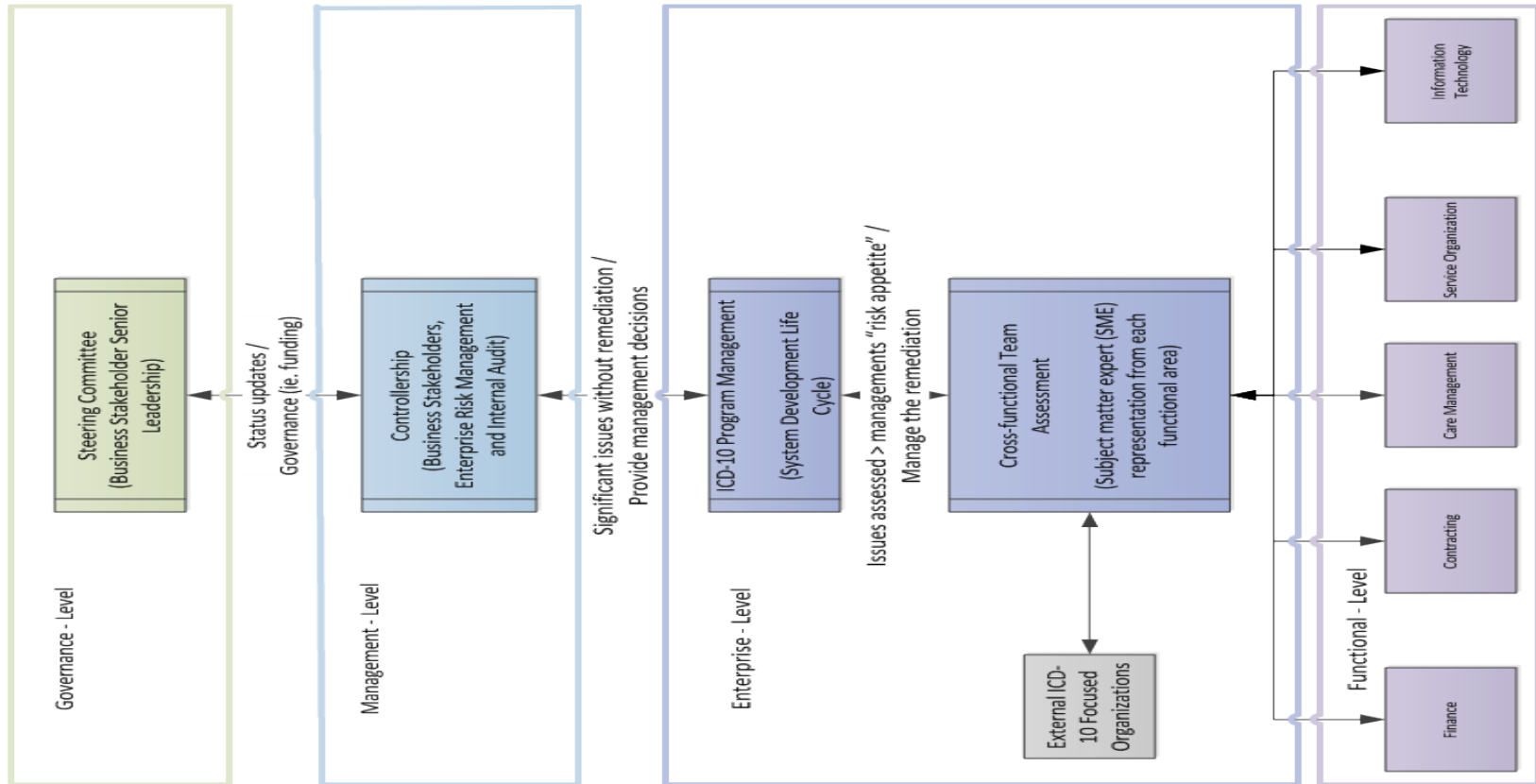
Appendix A

Functional Structure



Appendix B

Functional Structure



Presenter



ICD-10 Bio

D. Keith Hatch, CPA, CRMA
Florida Blue (Blue Cross Blue Shield of Florida)
Consultant Ib

Contact Information:

Work: 904.905.7543

Cell: 904.806.2710

ICD-10 Responsibilities:

Delivery Systems Business Lead

Provider Testing Lead

DS Operational Readiness Lead

Enterprise Operational Readiness Approach Team

WEDI: ICD-10 Transition Sub-Workgroup, Co-Chair

wediTM

