IT Governance

Checklist

For Hospital CIOs and IT Directors

The items in the following checklist reflect best practices in healthcare IT governance and represent several focus areas. It is not intended to be comprehensive, but answers to its questions should be a meaningful indicator of your IT department's performance.

Phoenix Health Systems

What is IT Governance?

IT governance is putting structure around how organizations align IT strategy with business strategy, ensuring that they stay on track to achieve their strategies and goals, and implementing effective methodologies to guide and measure IT's performance. An IT governance framework should answer key questions such as how the IT department is functioning overall, what ROI IT is providing the hospital, and – more than ever – how secure IT systems and information is from compromise.

The Information Systems Audit and Control Association has added another factor to this definition, mitigation of IT risks. **In healthcare, we often bundle risk mitigation with compliance, thus leading to these five focus areas for IT governance.**

1.Strategic management: Supporting the enterprise's objectives through linkages to IT objectives and activities.

2.Risk management and compliance: Developing and managing a formal risk mitigation framework that is HIPAA-compliant and sustainable, provides accurate and timely reports, is frequently updated to protect against new security risks, ensures that the organization complies with laws, standards, and best practices.

3. Efficient operations: ensuring that the varied day to day functions of your IT department are all working properly and in sync with each other.

4. Project management and value delivery: Focusing the IT department on value outcomes from the beginning of a project or investment and thereafter.

5.Resource management: Organizing your staff effectively and supporting its capabilities.

6. End user support and satisfaction: Ensures that there are quantitative and qualitative tools and processes in place to measure and report IT performance.

Strategic Management

What is IT strategic management?

Overall, it is a continuous process of strategic analysis, strategy creation, implementation and monitoring by the IT leader – as these activities relate to the strategic goals of the organization. The purpose of doing it is to leverage the capabilities of IT software, hardware and services to help enable (and prepare for) the organization's long- and short-term objectives.

The following page provides a best practices checklist.

Strategic Management Checklist

- ❑ The organization uses defined processes to manage the information technology (IT) operational area:
  - An approved Strategic Plan less than 2 - 3 years old.
  - An approved Tactical Plan less than 1 - 2 years old.
  - Strategic and Tactical Plans are aligned with the organization's objectives.
  - Policies and procedures are reviewed annually.
  - The project prioritization process is clearly defined and linked to strategic initiatives.
  - Network infrastructure is reviewed annually for technology obsolescence, stability, and ability to support newly approved technology projects.
  - The organization's network capacity plan is less than 1-2 years old and supports planned network growth estimates.

- ❑ Capital and Operational IT budgets have been developed and resources have been estimated and allocated for all major projects.

- ❑ A hospital IT Advisory Committee guides IT initiatives, making final decisions on IT projects, funding, and resource allocations.
  - The organization has a formal process to evaluate and approve major IT investments.
  - Organizational leaders / IT Advisory Committee are kept aware of developing technologies.
  - Clinicians are active participant in the IT Advisory Committee.
  - When evaluating new opportunities, the organization considers lessons learned from past IT projects.

- ❑ The CIO holds progress meetings with peers and key stakeholders at least quarterly.

Risk Management and Compliance

What is Risk Management?

Risk management is a straightforward process: simply addressing the priorities identified in your (recent!) risk assessment to develop a HIPAA-compliant roadmap that makes sense for your organization, based on its size, finances and other key factors.

The purpose of a HIPAA risk management plan is to provide a framework to evaluate, prioritize and implement measures to secure electronic protected health information (ePHI).

The plan must outline roles and responsibilities, methodical risk analysis and response planning. It must go beyond applying band aids, and include reasonably comprehensive protective measures and a process for monitoring, reporting, and controlling risks. It also is likely to include investing in tools for risk management, closing risks and identifying lessons learned.

Risk Management Checklist

- ❑ The IT department and/or Security Officer has conducted a HIPAA / HITECH security assessment within the last year and has a related, documented risk mitigation plan that it is acting upon.

- ❑ The organization has resolved all addressable and mandated HIPAA requirements, including employee training.

- ❑ The organization has formal IT security procedures, including procedures for reporting breaches.

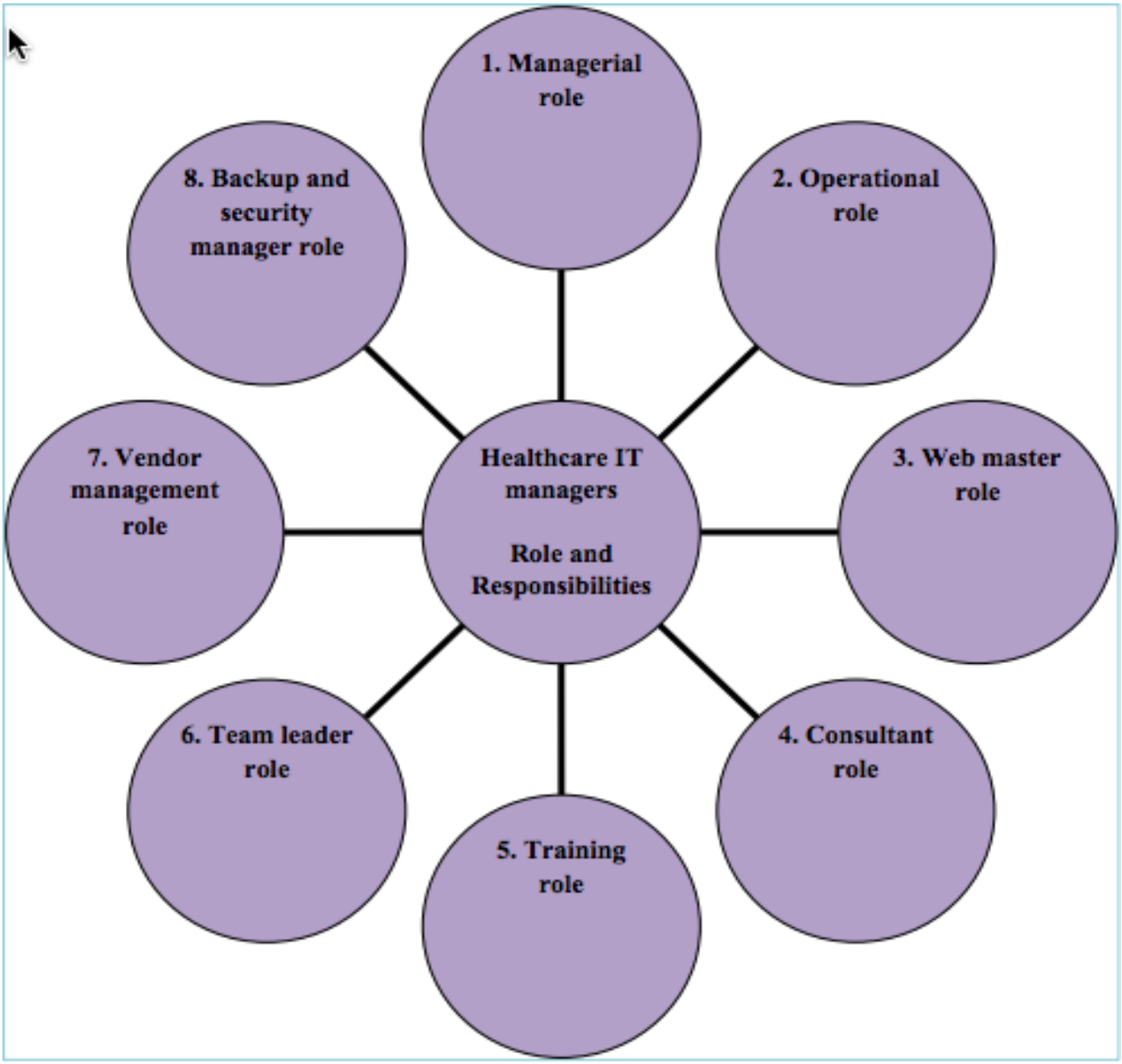
- ❑ The previous JCAHO inspection or other accrediting body gaps have been documented and corrective action completed.

- ❑ The organization has a forma, up to date IT disaster recovery plan.

- ❑ The IT disaster recovery plan is regularly tested, and appropriate staff have been trained on it.

- ❑ The company does regular intrusion detection and related monitoring and needed software and hardware updates.

Efficient Operations



IT Operations Center Checklist

- ❑ Conducts regular review to evaluate how current systems and applications are meeting the needs of the hospital and users.

- ❑ Coordinates with all department heads to receive input that may improve technology.

- ❑ Reviews the adequacy and allocation of IT resources in relation to funding, staff qualifications and performance, equipment, and service levels, for short-term needs and long-term goals.

- ❑ Has documented, detailed security processes for access to data center, and has prescribed backup processes.

- ❑ New software / hardware options are tested and adequately vetted prior to adoption.

- ❑ Has a formal process for measuring capacity and scheduling upgrades.

- ❑ Controls purchases, tracks and maintains licenses, and maintains technical and end-user documentation.

- ❑ Successfully implements the hospital's management systems, within budget and timelines.

- ❑ Manages a qualified help desk support staff that meets SLAs.

- ❑ Maintains strong knowledge of industry IT trends and new technologies.

Project Management and Value

- **Project management of IT related projects.**

  - There is a formal, industry standard methodology in place.
  - The methodology is used for all projects including status monitoring.
  - Standards for communication are established.
  - Budget vs. actual variances are documented & analyzed.
  - Post project evaluation are performed.

- **IT projects are tracked for return on investment (ROI).**

  - The organization has a formal process for measuring IT investment results post implementation.
  - A process for measuring accountability for results is in place.
  - A non-partisan review committee is regularly convened to review results & report findings.

Staff Resource Management

- ❑ IT positions are mapped to IT strategic plan and business initiatives.
- ❑ Goals and objectives are developed for each IT resource.
- ❑ An IT employee satisfaction survey is in place.
- ❑ A set of performance indicators for IT performance is regularly tracked and regularly reported.
- ❑ IT staff are provided regular needed training on new hardware, software, methodologies, controls, etc.

Ensuring Value Delivery Through End User Support

❑ IT support of end users.

- IT supports a help desk function with a formal service request methodology, KPIs, and SLAs (preferably ITIL-based).
- IT has a service request tracking system that tracks, collects and trends service request data, enables efficient knowledge base, and provides for client satisfaction surveys.
- The service request tracking system provides a customer feedback loop.
- IT has and uses a problem resolution methodology.
- IT analyses, identifies, and takes required action for end user application training needs.
- Backup, retention and restoring of service policies and procedures exist for end user created data (spreadsheets, word processing documents, etc.) stored on the corporate network.

❑ IT service level agreement (SLA) tracking.

- A documented process is in place to identify and track all items having an impact on customer service and end-user satisfaction
- There is a defined set of report parameters linked to SLAs
- Parameters are set for turnaround time for service requests. Examples include: (network, desktop, telecommunications, applications critical, same day, routine maintenance and/or problem solving).
- Parameters are set for network response time.

Are you sensing inefficiencies or even breakdowns in your IT department's performance? Perhaps it needs a "best practices" assessment or updating of its governance policies and procedures?

Phoenix Health Systems has over 20 years of healthcare IT consulting and outsourcing experience, and has managed many hospital IT departments. We offer the flexibility, energy and lower price points of a small company, and the expertise of a large company. We specialize in advising and supporting community and rural hospitals.

Contact us here:
https://www.phoenixhealth.com/contact/

Or email me personally:
D'Arcy Guerin Gue
Vice President Industry Relations
dgue@phoenixhealth.com

1130 East Arapaho Road,
Suite 500
Richardson, TX 75081
ph. 928-282-3038
contact@phoenixhealth.com

Phoenix
Health Systems