

Audit Assurance Professional
ITACS Program

Fox School of Business

Temple University

Philadelphia, PA 19454

Dear Student:

This audit engagement letter will confirm our understanding of the arrangements for your audit of the IT change management controls at CoreTec, Inc. (hereafter referred to as Company), for the quarter ending October 31, 2015.

You will review the Company's information technology change management process and related records, for the purpose of expressing an opinion on them. Proper IT change management processes are the responsibility of the Company's management. Your responsibility is to express an opinion on the effectiveness of the control.

You are to conduct your audit in accordance with the IS Audit and Assurance Standards and IS Audit and Assurance Guidelines issued by ISACA. Those standards require that you plan and perform the audit to obtain sufficient, relevant and valid evidence to provide a reasonable basis for the conclusion, opinions and audit findings (if any).

The procedure we provide includes tests of documentary evidence supporting the change transactions for the period and tests of the physical evidence.

We are aware that your audit is subject to the risk that material errors and irregularities, including fraud or defalcations, if they exist, will not be detected. However, we request that you inform us of irregularities that come to your attention, unless they are inconsequential.

You may not publish or otherwise reproduce our internal documents or records whether in part or in full.

You also agree to provide us with a copy of the final reproduced material for our approval before it is distributed.

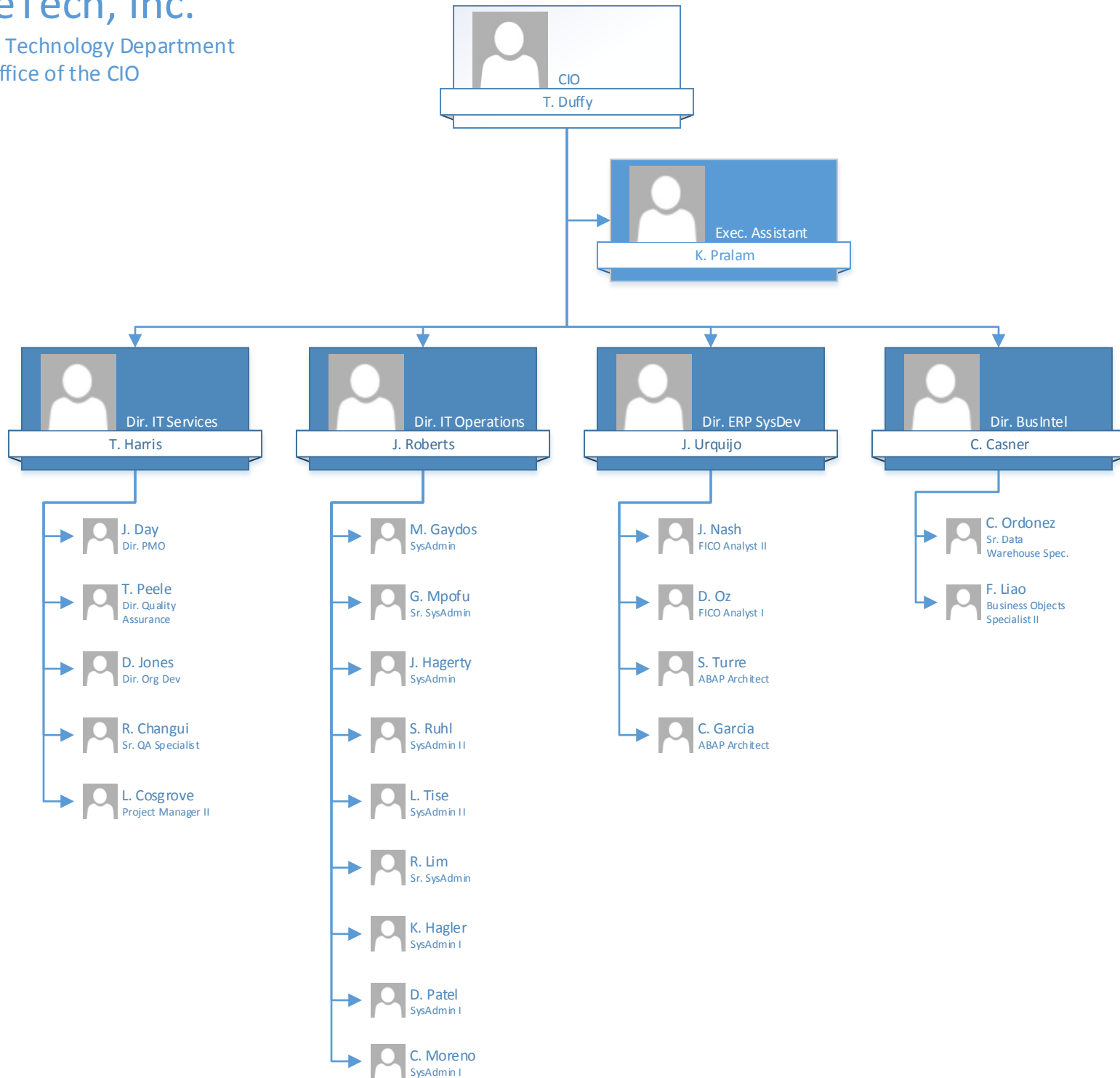
Sincerely yours,
Michael Romeu-Lugo
Adjunct Instructor

Approved By: Michael Romeu-Lugo

Date: November 15, 2015

CoreTech, Inc.

Information Technology Department
Office of the CIO



CoreTech, Inc. Internal Audit Assurance Program

IT Change Management

I. Objectives:

A. Control Objective(s):

Changes to the production environments are controlled in a manner that allows for fast and reliable changes while minimizing any risk that may impact:

- System integrity and stability
- Data confidentiality, integrity and availability
- The ability of the company to respond effectively to changing industry and regulatory environments.

B. Assurance Objective(s):

Before changes are promoted to production environments they must meet the following:

- The requested change must be approved by the Business Owner. The Business Owner is the head of the business area (or designee) responsible and accountable for the information managed by the system.
- All changes must be approved by the user.
- Promoting changes to the production environment must be performed by an appropriate system administrator.

II. Scope

Review of IT Change Management controls is performed on a quarterly basis. Changes applied during the period in scope will be reviewed.

III. Pre-audit Planning

A. Technical Skill(s):

- Working knowledge of IT Change Management processes
- Working knowledge of Windows, iOS, and UNIX environments, directory structures, and architecture
- Working knowledge of General Audit Software (Microsoft® Excel®)

B. Resource(s):

- Programming resources
- IT Business Analysts
- System Administrators
- Business Owners

C. Documentation:

CoreTech, Inc. Internal Audit Assurance Program

IT Change Management

- Current version of IT Change Management procedure(s)
- Listing of changes for the period

D. Location(s)

- Philadelphia Data Center

IV. Procedure:

A. Review Control

- Review the most current copy of the IT Change Management procedure. Make sure you understand the workflow, activities, and expected outcomes.
- Identify any required documentation and/or approvals required by the process.

B. Testing

- a. Sampling
 - i. Control Frequency: IT Change Management
 - ii. Sample Size: Entire Population
- b. For each unit in the population determine whether it was changed or not
- c. For each changed item:
 - i. Ensure that the change was properly authorized
 - ii. Find evidence of user acceptance testing
 - iii. Ensure that the change was promoted to production by a person with system administration access.

C. Communication

- a. Preliminary Findings – Report during engagement and Concluding Meeting
- b. Final Report and Recommendations – No later than 2 weeks after Concluding Meeting

CTI Change Management Policy

1 Purpose and Scope

This policy establishes management direction and objectives for IT change management and control. This policy enables fast and reliable delivery of changes to IT production environments, minimizing the risk of negatively impacting their stability or integrity of the changed environment.

The goals of this policy are the following:

- Authorized changes are made in a timely manner and with minimal errors.
- Impact assessments reveal the effect of the change on all affected components.
- All emergency changes are reviewed and authorized after the change.
- Key stakeholders are kept informed of all aspects of the change.

2 Definitions, Acronyms, Abbreviations

- **Change:** The addition, modification, or removal of approved, supported, or base-lined hardware, network, software, application, environment, system, or desktop build.
- **Emergency Change:** A change that must be introduced as soon as possible because of an unforeseen shortfall in an application, operating system, network, or hardware that requires immediate attention because of an existing or likely failure that will severely impact CTI's ability to conduct normal business operations.
- **Standard Change:** A change that is executed repeatedly, is of low risk to normal business operations, and is pre-authorized.

3 Roles and Responsibilities

- **Business Owner:** Person(s) responsible for the business process and supporting information systems.
- **Requester:** Person that submits a request for change.
- **System Administrator** – person responsible for supporting software applications and their environments.

4 Change Management Policy

It is the policy of the CTI Global IT organization to manage all changes in a controlled manner, including standard and emergency changes relating to applications and infrastructure.

All changes shall be:

- Approved by the Business Owner
- Appropriately tested and the results approved by the Requester prior to production use
- Promoted to production environment by personnel with appropriate system administration permissions.

4.1 Evaluate, Prioritize, and Authorize Change Requests

All change requests are to be evaluated to determine their impact on business processes and IT services, and to assess whether the change will adversely affect the operational environment and introduce unacceptable risk.

Changes are to be logged, prioritized, categorized, assessed, authorized, planned, and scheduled.

4.2 Manage Emergency Changes

Emergency changes are to be managed carefully to minimize further incidents, making sure the change is controlled, and takes place securely. Emergency changes are to be appropriately assessed and authorized after they are implemented in production.

CTI Change Management Policy

4.3 Track and Report Change Status

Change requests are to be managed in a tracking and reporting system to document rejected changes, communicate the status of approved, in-process changes, and complete changes. Tracking and reporting of change status help assure that approved changes are implemented as planned.

4.4 Acceptance Testing

Changes are to be tested independently prior to migration to production environments. The extent of tests and testing evidence must correspond to the risks associated with the change. Tests shall prove that change objectives are met.

User approval must be obtained before they are promoted to the production environments. Users should be involved in the design and execution of tests whenever possible.

4.5 Implement, Close and Document Changes

Changes are to be promoted to their final live environments once all testing, acceptance, and documentation activities have been completed. IT personnel shall provide confirmation that the migrated change operates according to specifications.

5 Enforcement

A breach of this policy could have severe consequences to CTI, its ability to provide products or services, or maintain the integrity, confidence, or availability of products or services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of CTI senior management. Severe, deliberate, or repeated breaches of the policy may be considered grounds for instant dismissal, or in the case of a CTI vendor or agent, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

6 References