**Boilerplate**

**Purpose**

* This is a “template” to be used as a “starting point” for the sake of helping you develop your own IT Governance Program.

**Copyright / Permission to Use**

* Permission to use this document is conditional upon you receiving this template directly from an **infotex** consultant, **infotex** website or e-commerce site, or an **infotex** workshop / training presentation.
* By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the “Transfer of Copyright Agreement” located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

**Instructions**

* Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
	+ All areas needing customization and/or consideration are in **red**.
	+ Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
	+ Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
	+ Sections in **green** are examples.
* Note that you should confirm that all text has been changed to “black” before considering this template final for your organization. If there are any sections in any other color than black, then all situations or customization has not been considered.

This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

# <Name of Financial Institution>Information Technology Tactical Plan2016, 2017, 2018

# Tactics for Implementing StrategyThis document presents the Information Technology Tactical Plan for implementing the Strategic Plan for <Name of Financial Institution>. The purpose of this plan is to provide a “roadmap” for the Information Technology Department to implement and deliver services that support the strategic mission and goals set by the bank.

# #1: Facilitate Tactical Plan of the Overall Bank Strategy

The technology plan must first and foremost facilitate the identified tactics from the bank-wide strategy. The following actions will accomplish this:

* Facilitate Confirmation Stages of Recent Technology Deployments
	+ Mobile Banking, Customer Relationship Management
	+ On-line Account Opening, On-line Loan Applications, Remote Deposit Capture
	+ Vendor Management, Business Continuity, Risk Management
* Facilitate Potential Change Management and New Technologies
	+ [Name Of Recent Compliance Issue] Compliance
	+ Dodd Frank Compliance
	+ Create and Maintain Designated Budget Lines for Operating and Capital Expenditures
	+ Facilitate new Marketing / Public Relations Strategy
	+ Facilitate the Pros/Cons analysis on forming a ERM Committee
	+ Facilitate potential addition of loan staff as well as routine replacement of existing staff
	+ Core Processing Contract Matures in 2018
		- Contracts expire June 2018
		- Prepare negotiation strategy
		- Integrate with Bank-wide Operating/Capital Budget
		- Prepare recommendations by mid-2016
		- Implement before July 2017
* Ensure systems will facilitate core deposit growth
	+ Use Mobile Banking and other technologies to help target a younger market segment, since like most banks, our customer base is aging.
	+ Make sure technology can facilitate our objective to develop other targeted market segments.
	+ Increasing business development efforts to increase our level of commercial DDAs. Continue offering Remote Deposit Capture, and monitor the effect of mobile banking on commercial DDAs.

# #2: Manage Technology Risk

The bank strategy is clear regarding the need to properly manage technology risk, including risk to customer information and the bank’s reputation. The following actions will accomplish this:

* Address the 2015 Audit Findings
	+ Major Finding #1
	+ Major Finding #2
* Five Steps of the Cybersecurity Assessment Tool
	+ Make sure management and the board reads Overview for Chief Executive Officers and the Board of Directors
	+ Make sure the IT Steereing Committee reads and understand the User Guide.
	+ Complete Part 1: Inherent Risk Profile
	+ Complete Part 2: Cybersecurity Maturity
	+ Interpret, Analyze, and Integrate Action Items into the 2016 Technology Plan
* Assist with the Bank-wide strategy of managing the following technology-related risks:
	+ Compliance and legal risk
	+ Strategic risk
	+ Reputation risk
	+ Customer Information System risk
	+ Non-Public Customer Information risk
* Continually Align IT Governance with the Bank’s Overall Strategy
	+ Investigate Hot Action Items from the Cybersecurity Assessment
	+ Inventory of Connections (plus add to Network Diagram)
	+ Investigate potential anticipated controls from GLBA/Technology Risk Assessment
	+ Implement next phase of Mobile Banking Tactical Plan
	+ Adjust IT Audit Plan to reflect any Hot Action Items gathered from the Cybersecurity Assessment
* Train Management Team on Triggers for Drill-down Risk Assessments
* Integrate Risk Management with Other IT Governance Programs
	+ Drill-down Risk Assessments for:
		- Secure Messaging
		- SIEM systems
		- Event Log Management: In-house or outsource?
	+ Summary of risk for ERM assessment

# #4: Training In All Directions

The bank strategy is clear that training is an important part of the overall strategy, and it is as important to the technology strategy. The new Cybersecurity Assessment Tool as well as recent audit findings also point to our Awareness Training Program as a primary tactic in both managing risk and aligning technology with business needs. Thus, we will be implementing the following tactics to bolster our training programs:

* **General:** According to bank strategy, <Name of Financial Institution> will invest in various training opportunities through trade association courses and seminars, regulatory, in-house, and other training. Technology Training will be directed at customers, vendors, employees, management, and board members, not to mention the members of the technology team itself.
* **Director Training:** According to bank strategy, training will need to be directed at Board Members as the new IT Governance Program is developed, as well as additional risk assessments are conducted. Overall Board Awareness Training focused on board responsibilities for technology risk management as per the FFIEC guidelines will be provided. As needed, policies and other documents will be presented to the Board with accompanying training information.
* **Bank Management:** The Information Technology Steering Committee will receive training centered around the Incident Response Plan, and various ad-hoc committee members will receive awareness training as part of the Risk Assessment updating process. The Information Security Officer will provide training as needed in order to assist the management team in the execution of various duties (such as vendor due diligence review, access authorization, data classification, etc.).
* **User Awareness Training:** As the end-user is the “first line of defense” in an Information Security Strategy, training for the user is paramount. The following will be utilized in order to facilitate adequate user-level awareness training:
	+ **Annual Acceptable Use Policy Training:** Each year, just after the Acceptable Use Policy is updated, all personnel who log into our network will undergo full training of the Acceptable Use Policy. This training will include a “due diligence exercise” which documents that the user not only received the training, but understood key provisions of the policy.
	+ **Awareness Reminders**: On a periodic basis, messages will be sent from the Information Security Officer related to specific current topics.
	+ **Awareness Activation**: Certain tests, walk-throughs, audits, etc. will be focused on measuring our ongoing awareness activation (are we on guard?) As new issues, vulnerabilities, or policies arise, the Information Security Officer will send via e-mail additional awareness reminders summarizing performance on tests meant to increase diligence.
	+ **New Employees:** As part of new employee orientation, the most recent Acceptable Use Policy Training and Due Diligence Quiz will be delivered.
* **Customer Awareness Training:** As we begin to comply with new regulations, increase the effectiveness of technology risk management, and find ways to further reduce overall security risk, we are seeing the need to develop a strong Customer Awareness Strategy. See tactical plan #5 below for more information.
* **Vendor Awareness Training:** As we improve upon our Vendor Management Program, various controls and requirements will be conveyed to various vendors depending on how much risk exposure our relationship with them creates. This information can be viewed as part of our overall awareness training program.

# #5: Finalize and Implement a Customer Awareness Strategy

Though already covered in tactical plan #4, we’ve never fully responded to the need for a cohesive, integrated Customer Awareness Strategy. The following actions will accomplish this:

* Finalize Customer Awareness Strategy
	+ Vulnerability Announcements
	+ Integrate into Customer Appreciation Events
	+ Impact Videos on Youtube page
	+ Facebook posts from infotex site
	+ Best Practice Training
	+ Mobile Banking Objectives
		- Integrate with Incident Response
	+ Broadcast Awareness Capabilities
	+ Integrate throughout all business processes
* Integration
	+ Marketing
	+ Social Media
	+ Retail Objectives
	+ Customer Service

# #6: Confirm 2015 Technology Projects

As part of our overall risk management process, and to respond to the strategy statement that we will confirm the effectiveness and planned return / risk mitigation benefits for all deployed technologies, the following actions will ensure appropriate closure of recent technology deployments:

For this, it’s usually easiest just to go through the last year’s tactical plan and pull out what you need to follow-up on (or what is not finished.) Sometimes looks like this:

**Switch Secure Messaging from Zix to Thru**

* Perform a “Post-mortem Review”
* Ensure access management issues are addressed.

**Mobile Banking Business Objectives**

* Perform a “Post-mortem Review”
* Ensure it meets our objective to retain and attract younger customers
* Ensure it meets our objective to grow our core customer base
* Ensure it meets our objectives to save time, transportation costs, and to ultimately improve operational efficiency.
* Integration with Other IT Governance Programs
	+ Customer Awareness Training
	+ Incident Response
	+ Cybersecurity Assessment Tool (if applicable)

 **Enhanced Telecommunications**

* Conduct post-mortem review of the Voice over IP project.

**Further Follow-up on Other Recently Deployed “Systems”**

* Instant Debit Card
* Board Portal
* Switch from Zix to Thru

# #7: Maintain High Regulatory Ratings

The bank’s strategy establishes a goal to maintain high regulatory ratings. To meet this strategy, we will:

* Review and improve the Audit Tracking System with the Internal Auditor
* Confirm closing of all audit items at least 30 days before next audit.
* Get an early start on the Request for Information coming from both auditors and examiners.
* Have the RFI Response ready ten business days prior to the on-site date.
* Provide a timely management response.

# #8: Facilitate Marketing / Advertising / Public Relations

The Bank will develop a formal marketing/advertising/public relations strategy by March 31, 2012. Technology should be considered in the development of this strategy not only from a new-technologies facility perspective (social media, in-branch communications) but also from a controls communication perspective (customer awareness training, incident response preparation, etc.)

To that end, the following objectives are in place:

* Facilitate risk management on new Web Site Design
	+ Investigate security risk with any interactive components
	+ Ensure appropriate content risk management
* Facilitate social media risk management.
* Integrate Marketing / Advertising / Public Relations with Incident Response Planning