**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.

# Technology Planning Policy LanguageConsider for our high level board policy

**Technology Planning:**The financial institution will take a formal, structured approach towards ensuring that information technology appropriately aligns with overall bank business strategy. A formal approach will also be taken regarding our approach to the adoption of new projects, products, technologies, services, and vendors.

### **Ad Hoc Technology Planning Team:**

On an <annual> basis, the <Technology Steering Committee / Business Planning Committee / Risk Management Committee> will convene an Ad Hoc Technology Planning Team to produce a Technology Plan which includes an update of the IT Strategy, IT Tactical Plan, and IT Budgets. It is essential that the Ad Hoc Technology Planning Team be multidisciplinary, include all members of the <Technology Steering Committee / Business Planning Committee / Risk Management Committee>, include membership from each business unit, and be given appropriate time to fulfill planning responsibilities.

**Technology Plan:**The Ad Hoc Technology Planning Team will assist the Information Security Officer in updating a Technology Plan Document that:

* Facilitates the successful achievement of all objectives articulated in the Business Plan.
* Includes a strategy for facilitating the business plan, and a separate, distinct tactical plan for meeting the strategy.
* Considers Risk Management Issues (open audit findings, risk assessment results, planned controls deployment, etc.)
* Considers new regulations and compliance requirements.
* Considers all known plans for new technologies, products, services, vendors, projects, and other planned changes.
* Renews the institution’s Adoption Philosophy.
* Renews the institution’s Risk Appetite.

**Adoption Philosophy**The Technology Plan will articulate the bank’s adoption philosophy in general, and the Information Security Officer will inform the Board of Directors whenever management strays from such philosophy.

**Risk Appetite**The Technology Plan will articulate the bank’s risk appetite in general, as it relates to technology deployment and strategic risk, as well as any residual risk related to new technologies, and the Information Security Officer will inform the Board of Directors whenever management strays from such appetite.

**Inventory of Tactical Plans:**To enable alignment of all IT Operations with the Business Strategy of the bank, the [Information Security Officer] will perform an analysis of all trends, new technology decisions, new projects, high-priority risk-mitigation, and other technology deployment plans, upgrades, integrations, etc. in the form of an overall inventory of potential and scheduled projects. The inventory will be updated and shared with the [IT Steering Committee / IS Steering Committee / IT Governance Committee / Audit Committee / EDP Committee] on a[n] [monthly/quarterly/semi-annual/annual] basis. The inventory should be treated as a structured agenda for discussing ongoing projects and upcoming trends on a regular basis. The discussion should center on strategy alignment, project ownership, status of projects, and where the financial institution wants to position itself in terms of technology adoption. The documentation should also identify timeframes for each issue in the inventory, using 6 month, 12 month, 18 month, and Next Technology Plan as the parameters.