Mobile use is justified when it has an efficient, positive impact on mission accomplishment. In applying mobile technology, users, information, and location must be considered.

Users: How do users accomplish the task now? How would use of mobile technology affect them?

Information: What is the source of the information? Is it government, public, or private data? What is its sensitivity?

Location: Where do the users need access to the information? How would mobile help?

Three dimensions influence selection of a mobility program. The constraints of this model include determining what capabilities are to be supported, how much the program can cost, and what degree of security is required.

As weight is increased in one dimension, each of the others is affected.

NIST SP 800-37 and 800-39 describe information security risk management as one aspect of a holistic organizational risk management program.

The mission benefits of implementing mobile computing must be weighed against risk to the organization, mission, information system, and to the Nation. The Risk Management Framework should be applied to the multiple facets of risk, which span legal, regulatory, policy, privacy, and technical domains.

Decision outcomes include the following: which applications, mobile devices, and types of infrastructure pieces are to be supported. Each decision outcome should be based on mission requirements, balance and trade-offs, and tailoring of risk.
Mobile Computing Decision Framework v1.0

**Mission Requirements**

How would mobile support the mission?

- Does mobile support my mission? (M1)
- Users (U)
- Information (I)
- Location (L)
- What is the mission impact? (M5)

**Decision Balancing**

How shall I weight the dimensions?

- Capabilities (B1)
- Security (B3)
- Economics (B2)

**Risk-Based Tailoring**

How will I cover the various risks?

- Financial (T1)
- Security (T7)
- Policy (T2)
- Privacy (T6)
- Technology (T4)
- Legal (T3)
- Operations (T5)

**Results**

Selecting the right solution

Evaluation and Assumptions

Briefly describe your mission and the use-case you are evaluating for mobile technology.

Use the diagram above to place a dot where you believe your balance is. Take note a shift toward one dimension may result in a loss in others.

Assign a confidence rating in each of the circles above where you feel you have tailored your mobile solution to those risks. Circle that number in the chart below for each risk consideration.

The evaluations, assumptions, and decisions from the worksheet should lead you to a general idea of the mobile solution appropriate for your mission, priorities, and risk tolerance.

Decisions

What are the elements of your mission requirement from above?

- M1. Does mobile support my mission?
- M2. Who are the users involved?
- M3. What is the source and sensitivity of your information?
- M4. Where will the information be needed by the users?
- M5. What is the mission impact?

What are the factors influencing your balance above?

- B1. Capabilities
- B2. Economics
- B3. Security

How confident are you that risk has been adequately addressed?

- Financial (T1)
- Security (T7)
- Policy (T2)
- Privacy (T6)
- Technology (T4)
- Legal (T3)
- Operations (T5)

What solution aspects make sense?

- R1. Application
- R2. Device
- R3. Infrastructure

To Dos or “What don’t I know?”
Mobile Computing Decision Framework

**Mission Requirements**

- How would mobile support the mission?

**Decision Balancing**

- How shall I weight the dimensions?

**Risk-Based Tailoring**

- How will I cover the various risks?

**Results**

- Selecting the right solution

---

### Evaluations and Assumptions

- Due to budget cuts, evaluating to reduce overall mobile device costs through two-pronged approach:
  1. Optimize rate plans for agency provided mobile devices, and
  2. Implement a BYOD pilot program.

- Non sensitive data. No PII.

- Everywhere the employee is, including on site. Currently looking to provide wifi hotspots at work locations.

- Efforts will create efficiency for agency and save money.

### Decisions

- **M1. Does mobile support my mission?**
  - Yes, it enables work communication via email and phone to 550 employees

- **M2. Who are the users involved?**
  - Employees and Executives

- **M3. What is the source and sensitivity of your information?**
  - Government email, no sensitive/PII: government on-premise, cloud, with the employee

- **M4. Where will the information be needed by the users?**
  - On-premise, alternative work locations, with employees

- **M5. What is the mission impact?**
  - Positive: Reevaluating mobile needs to enable work communication will reduce cost, thereby, meeting budget goals

---

### Evaluations

- **Capabilities (B1)**
  - Email and Voice - Notifylink MDM (cloud product)

- **Security (B3)**
  - Minimum security. Limited security functionality. Note: No PII, no real data sensitivity

- **Economics (B2)**
  - Bundle mobile data/voice packages and offer BYOD ($120 per year per user plus $5 per year for applications)

- **Financial (T1)**
  - Top priority - Cost reduction is the driving factor to meet budget constraints and enable mission

- **Policy (T2)**
  - Require users to sign acceptable behavior policy, update security policies pertaining to mobile device

- **Legal (T3)**
  - Minimal addressed. Reimbursement unclear

- **Technology (T4)**
  - Addressed

- **Operations (T5)**
  - Addressed

- **Privacy (T6)**
  - Addressed. No PII

- **Security (T7)**
  - Minimal addressed. Password lock required on device; password complexity and aging enforced for email

---

**Application (R1)**

- Applications: Provide support for GWMail and GWCalendar

**Device (R2)**

- Device: Initiate BYOD alpha pilot and maintain Blackberry support as needed

**Infrastructure (R3)**

- Infrastructure Transport: Do not support or limit any transport for BYOD. Business as usual for Blackberry use

---

**Example Case Study**

- **Low — Level of confidence — High**

---

**Mobile Computing Decision**

From: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs