Security and governance strategies for the consumerization of IT

Microsoft recommendations for a consumerization of IT strategy

Abstract:
Considerations about security and data management are central to discussions about consumerization of IT strategies. Further, governance planning for such strategies must address not only security issues, but also the appropriate usage of devices, and support for corporate services on user owned devices.

Microsoft Services

Author:
Arno Harteveld, IP Development Architect, Microsoft Services

Publication date:
April 2012

Version:
1.0

We welcome your feedback on this paper. Please send your comments to the Microsoft Services Enterprise Architecture IP team at ipfeedback@microsoft.com.
Document readership:
This white paper is intended for a high-level, non-technical audience of business/IT decision makers and stakeholders from human resources, finance, legal, and other business areas. This white paper supports Microsoft enterprise architects who participate in strategic discussions regarding consumerization of IT initiatives, and provides intellectual property content that may be excerpted, customized, and reassembled as appropriate.

Acknowledgments
The author wants to thank the following people who contributed to, reviewed, and helped improve this white paper.

Contributors:
Brian Seitz, David Tesar, Rob Tiffany

Thanks also to:
Stella Chernyak, Susan Conway, Ulrich Homann, Jeff Johnson, Eduardo Kassner, Bryan McMillan, Robert Standefer

© 2012 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement.
# Table of Contents

1 OVERVIEW ...................................................................................................................... 1

2 SECURITY STRATEGIES FOR “BRING YOUR OWN” DEVICES............................................. 2

2.1 SECURITY LAYER CONCERNS ....................................................................................... 3

2.1.1 Location concerns ................................................................................................. 3

2.1.2 Network security concerns ................................................................................... 3

2.1.3 Unmanaged device concerns ................................................................................. 4

2.1.4 Application concerns ............................................................................................ 5

2.1.5 Data concerns ....................................................................................................... 5

2.2 TECHNIQUES THAT SUPPORT SECURITY STRATEGIES .................................................. 5

2.2.1 Containerization techniques .................................................................................. 6

2.2.2 Virtualization techniques ..................................................................................... 6

2.2.3 Encryption techniques ......................................................................................... 6

2.2.4 Protecting data and corporate resources ............................................................... 7

2.2.4.1 Identity and access management .................................................................... 7

2.2.4.2 Digital asset qualification ............................................................................... 7

2.2.4.3 Platform security ............................................................................................ 8

3 GOVERNING A CONSUMERIZATION OF IT STRATEGY ........................................................... 10

3.1 LANDING STRATEGY IN THE ORGANIZATION ............................................................... 10

3.2 “BUSINESS FIRST” STRATEGY: DEFINE POLICIES THAT EMBRACE THE CONSUMERIZATION OF IT .......................................................................................... 10

3.3 CONSUMERIZATION OF IT POLICY AREAS ............................................................. 11

3.4 ADOPTING A MULTIDIMENSIONAL DEVICE POLICY ............................................... 12

3.4.1 Mixed ownership .................................................................................................. 12

3.4.2 Device policy drives management policy ............................................................... 12

3.5 DEFINING A MANAGEMENT POLICY ........................................................................... 14

3.5.1 Defining access policies ....................................................................................... 15

3.5.2 Delivering services to devices ............................................................................. 16

4 REFERENCES ..................................................................................................................... 19
1 Overview

Consumerization of IT introduces the notion of unmanaged devices, also referred to as untrusted platforms. When planning for the consumerization of IT, enterprises must develop strategies to mitigate risks and protect sensitive assets, and develop policies for information protection, data management, platform security, and other related areas. This white paper discusses security and governance strategies that help mitigate risk.

This white paper is one part of the “Microsoft Recommendations for a Consumerization of IT Strategy” series. This series introduces the phenomenon known as the consumerization of IT, including strategies for supporting the proliferation of devices in the workplace, and supporting work tasks on personal devices at diverse locations.

The full list of white papers that comprise this series is:

- “How to build a consumerization of IT strategy”
- “Considerations for a successful consumerization of IT architecture”
- “How the consumerization of IT affects your business”
- “Security and governance strategies for the consumerization of IT” (this paper)
2 Security strategies for “Bring Your Own” devices

The following strategies for addressing security issues are useful in environments that support the consumerization of IT:

- **Containerization.** Encapsulation of digital assets. Putting digital assets into an isolated location establishes a context for managing information that is distinct from the underlying device and operating system.
- **Virtualization.** Isolation of digital assets or infrastructure services. Isolation establishes a distinct context and resource pool.
- **Encryption.** Encryption protects digital asset from unauthorized access and tampering. Encryption is used in combination with containerization and/or virtualization.

The following figure illustrates the relationship of these security strategies.

![Figure 1. IT security strategies applicable to the consumerization of IT](image)

These strategies help mitigate risk across all the layers of the security model, as shown in the following figure.
Some security risks can be mitigated by using technologies, whereas others can be mitigated by applying a management policy. The “Security layer concerns” section of this paper discusses governance and policy design.

2.1 Security layer concerns

Concerns at the security layer include those associated with location, networks, devices, applications, and data.

2.1.1 Location concerns

As people, devices, and data become mobile, people may have access to confidential information at any time and any place. Policies must be defined to raise awareness of risks, such as those that could be presented when an employee chooses to look at customer financial data while at a coffee shop. In addition, access to information can be blocked by a technical infrastructure that senses the location of a user and adapts corporate services as appropriate.

2.1.2 Network security concerns

Potential risks are involved when devices connect to corporate infrastructure (public, private, and cloud), as show in the following table.
Table 1: Network security concerns

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network sniffing or data hijacking</td>
<td>Containerization, Virtualization, Encryption</td>
</tr>
<tr>
<td>Malware contamination of infrastructure</td>
<td>Not applicable, Network virtualization, Data encryption, Network encryption</td>
</tr>
</tbody>
</table>

2.1.3 Unmanaged device concerns

The consumerization of IT introduces challenges such as having both employee-owned and business-owned devices within the same network, and allowing different management levels for these different devices. The follow table summarizes specific concerns for unmanaged devices.

Table 2. Unmanaged device concerns

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown health state of unmanaged devices and/or operating system.</td>
<td>Containerization, Virtualization, Encryption</td>
</tr>
<tr>
<td></td>
<td>Not applicable, Network virtualization, Data encryption, Network encryption</td>
</tr>
</tbody>
</table>

Unmanaged devices can introduce the following device-related risks:

- Unknown health state of device which can lead to the risk of malware distribution
- Operating systems tampering—for example keyloggers, rootkits, and device unlocking such as, jail breaking, device unlocking.
- Unauthorized data disclosure

Table 3. Risks with deploying corporate apps on unmanaged devices

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure contamination by malware distribution</td>
<td>Containerization, Virtualization, Encryption</td>
</tr>
<tr>
<td>Application containerization</td>
<td>Operating system virtualization, App virtualization, Network virtualization</td>
</tr>
<tr>
<td>Application sandboxing</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Managed devices, whether privately owned or owned by the business, can introduce risks related to exposing data and applications on inappropriate platforms. These include:
• Personal applications on corporate devices
• Personal data on corporate devices
• Corporate applications on personal devices
• Corporate data on personal devices

2.1.4 Application concerns

Running applications on unmanaged devices can lead to the risk of tampering with application executables or associated application data or settings (for more information, see the “Platform security” section). A number of measures can help applications survive within hostile environments, as shown in the following table.

Table 4. Application concerns

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application tampering</td>
<td></td>
</tr>
<tr>
<td>Containerization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Application containerization</td>
<td>Application virtualization</td>
</tr>
<tr>
<td>Application sandboxing</td>
<td>Application obfuscation</td>
</tr>
<tr>
<td></td>
<td>Application signing</td>
</tr>
</tbody>
</table>

2.1.5 Data concerns

Storing data on unmanaged devices exposes the data to the risk of unintended disclosures. Information classification can assist in understanding the consequences of information disclosure (for more information, see the “Protecting data and corporate resources” section). A number of measures can be applied to protect data (for more information, see the “Platform security” section).

Table 5. Data concerns

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to corporate data</td>
<td></td>
</tr>
<tr>
<td>Containerization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Storage container</td>
<td>No local data storage but remote access to data by desktop or application virtualization.</td>
</tr>
<tr>
<td></td>
<td>Content encryption</td>
</tr>
<tr>
<td></td>
<td>Storage encryption</td>
</tr>
</tbody>
</table>

2.2 Techniques that support security strategies

The consumerization of IT is driving the development of many security strategies, including the most common approaches described in this white paper: containerization, virtualization, and encryption. This section discusses these techniques further.
2.2.1 Containerization techniques

Containerization involves encapsulating digital assets (data or applications) and separating them from the underlying device and operating system with the goal of protecting the assets. Containerization includes the following areas:

- **Storage containers.** Provide secure data storage for corporate data.
- **Application containers.** Provide secure contexts for corporate applications, including secure application communication channels to corporate resources.
- **Application sandboxes.** Provide secure contexts for corporate applications, including secure application communication channels to corporate resources.

2.2.2 Virtualization techniques

Virtualization involves separating resources between different layers of the security model, as follows:

- **Hypervisor.** Separation of the operating system from the underlying device.
- **Desktop virtualization.** Separation of the desktop from the underlying operation system. Desktop virtualization can use technologies such as remote pixel projection.
- **Application virtualization.** Separation of applications from the underlying operation system through application virtualization (locally) or pixel projection (remotely).
- **Network segmentation and network gateways.** Separation of network infrastructures through virtual networks. Access to network segments is granted based on user identity and compliance with management policies.

2.2.3 Encryption techniques

Encryption techniques protect digital assets and IT services from unauthorized access and tampering. Encryption is used in combination with containerization and virtualization.

Encryption techniques can be applied on a per-user or a per-device basis, using controls at the operating system level such as certificate-based identity management.

Encryption is useful for protecting the following digital assets:

- Stored data is protected with device storage encryption.
- Documents are protected with content encryption such as digital rights management.
- Data in-transit is protected with network encryption provided by protocols, such as virtual private network (VPN) or HTTPS.

Device-specific security capabilities must be considered when conducting an initial assessment of risk and implications to the infrastructure. For example, devices may have the ability to support end-to-end encryption, but require a customer to purchase additional infrastructure services to enable this feature.

Most enterprises have requirements that include knowing that:

- Data at rest is safe, no matter where it lives
- Data is safe in transit
- Personal devices do not put internal systems at risk
- Information assets on personal devices can be recovered, if necessary
- Lost devices do not compromise confidential data

A consumerization of IT strategy can address information protection requirements after:

- Assessing information risk based on nature of business, geographic spread, and organization culture
- Creating a risk map and deployment plan that outlines required IT training and employee awareness programs
2.2.4 Protecting data and corporate resources

The “Identity and access management” section provides an overview of components of a security infrastructure and considerations related to the consumerization of IT. It is essential to engage device suppliers to determine how the following areas will be addressed to support the security goals of the enterprise.

- **Encryption solutions.** On mobile devices and between apps and the corporate network.
- **Data management and data loss prevention (DLP) solutions.** Deploying tools for data management and recovering or wiping lost data from lost devices.
- **Virtualization and Remote Desktop Services.** Improving scalability and overall utilization of the consumerization of IT infrastructure by centralizing administration; rendering remote view of desktop to avoid data stored on device itself.
- **Identity and access management.** Managing user life cycle and access management on mobile devices.

### 2.2.4.1 Identity and access management

The process of determining and validating a user’s identity is referred to as **authentication**. The process of managing a user’s level of access to various resources is called **authorization**.

Operating systems typically implement a set of authentication protocols as part of an extensible architecture (for example, Kerberos, passwords, claims-based, and certificate-based). These protocols and packages enable the authentication of users, computers, and services. The authentication process, in turn, lets authorized users and services access resources in a secure manner.

Platforms should provide the following capabilities to implement and enforce user credentials and password controls for applications, databases, and server and network infrastructure:

- User identity verification prior to password resets
- Timely access revocation for terminated users
- Remove or disable inactive user accounts
- Password expiration capability
- Minimum password length and strong passwords policy enforcement
- User ID lockout capability
- Maintain user activity logs for privileged access or access to sensitive data
- Multi-factor authentication is usually implemented for all remote user access (for example, by using smart cards and digital certificates as described in the following section)

Typically, operating systems also implement interoperable security mechanisms to provide security measures that integrate across the various systems on the networks they manage. That is, certificate-based identity management and authentication and authorization functionality.

### 2.2.4.2 Digital asset qualification

One of the key elements of establishing a consumerization of IT strategy is the need to govern access to digital assets (such as services, apps, and data) that have a variety of levels of sensitivity.

As a first step toward managing digital assets, enterprise assets must be classified based on the impact of unintentional disclosure. The greater the value of the asset, the tighter the security controls of the
access policy. Within the IT industry, there are a number of standards with regards to information classification such as: ISO 27001/ISO 27002\(^1\) and NIST SP800-53r3\(^2\).

Microsoft has adopted a four-level information classification system for assets that includes:

- **High business impact (HBI).** Information assets that, if disclosed without authorization, could cause severe or catastrophic material loss to the information asset owner or relying parties.
- **Moderate business impact (MBI).** Information assets that, if disclosed without authorization, could cause serious material loss to the asset’s owner or relying parties.
- **Low business impact (LBI).** Information assets that, if disclosed without authorization, could cause limited or no material loss to the asset owner or relying parties.
- **Public data.** Information assets that are publicly available without authorization.

### Protecting sensitive data

Sensitive data protection refers to how your application handles any data that must be protected either in memory, over the network, or in persistent stores. Sensitive data protection measures include:

- **Secure access to data sources.** Consumerization of IT processes should use secure mechanisms to connect to and extract data from source systems, and access only the data that is relevant to the current process.
- **Secure storage of data.** After the data has been extracted from the source systems and loaded into a centralized database, the database storage method might facilitate unauthorized access to data. For example, an unauthorized user would only need to break into one system instead of many to gain access to the data. Therefore, it is important to secure access to the centralized database server.
- **Secure transit and local storage of data.** The system should use encryption when transmitting highly sensitive data over the network or caching that data locally on a client computer.
- **Personally identifiable information or private data.** If you show or distribute information that might identify an individual, determine where and how the information is collected, transmitted, and displayed, and take steps to ensure that it is secure.
- **Secure password secrets.** The design identifies the methodology to store secrets securely and secrets are not stored unless necessary.

### Input and data validation

Provide a valuation mechanism or process to protect against common threats such as buffer overflow, cross-site scripting, and SQL injection. Perform a detailed security review to identify any weaknesses in the validation of data input that could allow malicious access and back door attacks.

#### 2.2.4.3 Platform security

Areas of interest to the larger topic of platform security include session management, communication security methods and models, configuration management, exception management, and auditing and logging.

---

Session management
A session refers to a series of related interactions between a user, a device, an application or a web browser. The security design should identify how to handle and protect user sessions as follows:
- Session lifetime is defined and limited
- Session state is protected from unauthorized access, using encryption or a secure channel
- Session identifiers are not passed in query strings

Communication security methods and models
Unprotected information exchange across the Internet, extranets, intranets, and between applications presents potential security risks. Challenges include preventing unauthorized parties from eavesdropping on data during transport, impersonating an authorized user, or disrupting services.

Configuration management
Configuration management refers to how a solution handles operational issues, such as how solution components run, which databases they connect to, how they are administered, and how they are secured. Considerations include the following:
- Ensure that administration interfaces are secured (use strong authentication and authorization) as well as remote administration channels.
- Verify that configuration stores are secured and configuration secrets are not held in plain text in configuration files.
- Use least-privileged process accounts and service accounts.

Exception management
Exception management protects against denial of service attacks and the disclosure of sensitive system-level details. The security design should outline a standardized approach to structured exception handling across devices and applications and identify generic error messages that are returned to the client to minimize the disclosure of information in the case of an exception.

Auditing and logging
Auditing and logging refer to how your infrastructure records security-related events. Security design identifies the level of auditing and logging necessary for the application and identifies the key parameters to be logged and audited.

The design considers how to flow caller identity across multiple tiers, at the operating system or application level. For auditing, use an auditing setting that logs all logon attempts by recording the event in the system log. For example, in Windows operating systems, the Windows Event Log is the mechanism for tracking logged events.
3 Governing a consumerization of IT strategy

Clients face a number of governance-related challenges with the introduction of a consumerization of IT strategy. These include:

- Support for mixed ownership and mixed support modes
- Licensing and policy changes for consumer device vendors
- Region-specific legal and insurance procedures

Failing to comply with regulations is one of the greatest challenges for organizations that are adopting or managing enterprise-wide consumerization of IT strategies. The types of questions that must be considered include:

- How can I ensure that employees do not send sensitive data from their own devices?
- What if employees post sensitive data on social media sites?
- What happens when an employee’s unsupported device malfunctions?

3.1 Landing strategy in the organization

The goal of a strategy is to achieve an outcome that benefits the organization. This requires decision making at a senior level, then using a process to implement changes, and adapting governance within the organization. To support strategy, policies and related concepts are clearly defined in distinct but interrelated ways. These include:

- **Policy.** General statement of principle that changes infrequently. Policies are applied enterprise-wide and are approved at the senior level of the organization.
- **Standards.** Requirements and controls for accomplishing policy using detailed processes that require conformity.
- **Procedures.** Methods for complying with standards using step-by-step processes according to instructions and forms.
- **Guidelines.** Best practices that are encouraged, but not required. This category includes helpful hints, tips, and user guides.

3.2 “Business first” strategy: Define policies that embrace the consumerization of IT

The demand for innovative and privately owned devices is driving changes to enterprise policies, management policies, and the underlying infrastructure that supports those devices.

Enabling a consumerization of IT strategy requires a rethinking of policies, which must fulfill business objectives given the constraints of IT services and consumer devices.

![Figure 3. Policy is informed by both business objectives and enterprise constraints](image)

Discussions of policy form a critical foundation for the consumerization of IT, which covers different policy categories. Policies need to be tiered to address differing combinations of devices and enterprise services, while addressing security considerations.
Enterprise architects can help define policies that support strategic objectives by guiding the discussion using the following policy categories:

- **Device policy.** Establish guidance on utilizing devices in the enterprise.
- **Management policy.** Establish criteria or standards to support the use of IT services on devices.
- **Access policy.** Establish guidance for accessing and utilizing corporate information assets.

These categories of policy are interdependent, producing an overall policy for consumerization of IT within an enterprise, as shown in the following figure.

![Policy diagram](image)

**Figure 4. Interaction of policy categories**

### 3.3 Consumerization of IT policy areas

When implementing a consumerization of IT strategy, an enterprise will need to:

- Revise (technology) policies and quality controls that mitigate risk.
- Jointly develop new policies with appropriate business units, including IT, human resources, finance, and legal.
- Ensure the enterprise meets compliance and financial requirements.

The major areas that consumerization of IT policies cover include policies related to devices, management, access, security, and support.

- **Device policies:**
  - Supported and unsupported hardware and software.
  - Employee responsibility to have a suitable computer or device available for company use at all times. This policy area includes the minimum specifications for the hardware and operating system that the employee uses. These details also include purchasing responsibility and budget for hardware, software, and third-party support.

- **Management policies:**
  - Enforcing configuration of the devices.
  - Asset usage tracking (devices and applications)

- **Access policies:**
  - Remote-access policies
  - Levels of permissible access to data

- **Security policies:**
  - Safe storage of company data

- **Support policies and procedures:**
  - Protocols to follow if a device is lost or stolen.
  - Protocols to follow when an employee is terminated, such as cleansing data from a notebook hard drive, or resolving financial liabilities for the enterprise and employee.
3.4 Adopting a multidimensional device policy

The consumerization of IT forces enterprises to move from a single device policy, where the business provides everything, to a multidimensional device policy that has a mixed ownership and management model.

When defining and adopting such device policies, key questions to consider include:

- What kind of device can you bring to the office for work?
- What kind of device can you connect to the network for work?

3.4.1 Mixed ownership

Each ownership option may include a range of possible device types, some applicable to more than one ownership option.

![Figure 5. Device types and ownership](image)

Moving to a policy that addresses mixed ownership impacts the following areas of an enterprise:

- Device choice
- Device support policy (software or hardware failure, device theft)
- Device management
- Information access
- Finance (software licensing, device purchasing)
- Legal (ownership of data on the device)

3.4.2 Device policy drives management policy

In consumerization of IT initiatives, device policy drives device management policy. This is a reversal of the circumstance that many IT departments address: defining policies for device usage based on management policies.

For IT to become an enabler for supporting new consumer and enterprise devices, the organization must develop management, security, and health policies that align with device attributes and IT service capabilities. Different devices will likely have different policies, and policies can include user location and type of connectivity.
For example, the following table describes options based on a range of management, access, and security features. The resulting alignment of policies creates the categories for “corporate,” “partial,” “proxied,” and “public.”

<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>Proxied</th>
<th>Partial</th>
<th>Corporate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>• Consumer</td>
<td>• Remote Secure</td>
<td>• Enterprise Mobile</td>
<td>• Enterprise Compliance</td>
</tr>
<tr>
<td>Security</td>
<td>• User-managed • Local admin</td>
<td>• Enterprise managed • Authentication</td>
<td>• Enterprise managed • Authentication (password required for device access) • Remote wipe</td>
<td>• Enterprise managed • Authentication (password complexity, smartcard) • Storage encryption • Corporate &amp; Device Policies • Audit trace and logs</td>
</tr>
<tr>
<td>Health</td>
<td>• User-driven health management</td>
<td>• N.a.</td>
<td>• Health assessment • Patch, firewall, configuration</td>
<td>• Health enforcement • Patch, firewall, configuration • Device policies</td>
</tr>
</tbody>
</table>

**Figure 6. Management and security options**

Each policy collection (such as proxied) is mapped to at least one device category (such as Bring Your Own) and each device category can support multiple policies. For example, a smartphone may use a proxied policy when at the home of the user, and a partial policy when at the business location and connected to the corporate network.

Devices are governed based on policies that depend on the device attributes and policy compliance. For example, device attributes may include content protection (using drive encryption) and policy compliance may include a device that is managed by a management agent that the user installs on a device. In this way, it is up to users to decide the kinds of policy they are willing to accept, and the consequent services they are allowed to consume on their devices.

For example, the following chart shows multiple device options associated with the previously defined policy collections, each of which is composed of access and health policies (described in the “Defining a management policy” section).
3.5 Defining a management policy

A consumerization of IT management policy covers “access policy” and “health policy” and their subcategories.

Access policy includes sub-policies that govern:
- Device access
- Information access
- Network access

Health policy includes sub-policies that govern:
- Device integrity
- Operating system integrity
- Application integrity

The following table shows examples of these policies and methods used to mitigate associated risks.

Table 6. Aspects of management policy

<table>
<thead>
<tr>
<th>Policy Aspect</th>
<th>Policy Subcategory</th>
<th>Protection Mechanism</th>
<th>Mitigated Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Device Access</td>
<td>Device protection through authentication</td>
<td>Unauthorized access to the device</td>
</tr>
<tr>
<td></td>
<td>Information Access</td>
<td>Content protection through encryption</td>
<td>Disclosure of confidential content, such as documents and email</td>
</tr>
</tbody>
</table>
### 3.5.1 Defining access policies

Access policies are components of management policy. Access to data must accommodate information that has a variety of levels of sensitivity, accessed on a range of devices from differing locations, as described in the “Digital asset qualification” section.

For example, a “corporate” management policy can permit access to confidential customer data, while a “proxied” management policy may only allow access to information about current product offerings.

Data classified using the four-level system in use at Microsoft (high business impact [HBI], moderate business impact [MBI], low business impact [LBI], and public) can be associated with management policies as described in the following table.

<table>
<thead>
<tr>
<th>Table 7. Management policies and access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Policy</strong></td>
</tr>
<tr>
<td>Corporate</td>
</tr>
<tr>
<td>Partial</td>
</tr>
<tr>
<td>Proxied</td>
</tr>
<tr>
<td>Public</td>
</tr>
</tbody>
</table>
Although the specific correlation of data sensitivity to management policies will differ among enterprises, there will generally be a need for a tiered service structure. The following diagram illustrates a tiered alignment of information access policies with management policies.

Figure 8. Aligning management policies with asset classification

3.5.2 Delivering services to devices

The benefits of the consumerization of IT are realized when IT delivers services that support the business to consumer devices. For example, such services could include providing sales application features to devices that deliver current sales and customer data while on-site at customer locations.

**Note**  For more information about relevant scenarios, see the companion white paper: “How the consumerization of IT affects your business.”

To determine the types of services and information that can be provided through a specific device category, digital assets must first be classified, and IT needs to define a service portfolio that aligns applications and services to the management policies and device policies. An example of service alignment to management policy is shown in the following diagram.
Figure 9. Align services with management policy

To support service delivery, application features need to be adapted to the limitations (display size) of the device, as well as the user experience (touch, gesture, and speech). The provided feature set must also be adapted to address concerns around risk and compliance, but should still provide a compelling experience for mobile workers.

The following table presents examples of the types of services that IT can provide to mobile devices subject to different management policies.

Table 8. Examples of services that IT can provide to mobile devices

<table>
<thead>
<tr>
<th>Management Policy</th>
<th>Services</th>
</tr>
</thead>
</table>
| **Corporate**     | Full-access to all corporate applications such as line-of-business applications, business intelligence, and ERP apps.  
Confidential information (HBI) can be stored on devices that comply with this policy. 
Devices with extensive security feature sets, such as storage encryption and secure device access, are compliant to this management policy. 
Includes all services provided through partial, proxied, and public policies. |
| **Partial**       | Access to corporate applications that provide MBI classified information and services are typically provided for this management policy. 
Documents that contain confidential information (MBI) are encrypted and can be stored on the device. 
Devices that have a less extensive security features may be out of compliance with corporate management policy and need remediation by applying updates available under this policy. |
<table>
<thead>
<tr>
<th>Management Policy</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile apps adapted to multiple form factors, such as email, calendaring, CRM, and ERP applications.</td>
<td></td>
</tr>
</tbody>
</table>
| **Proxied** | Access to proxied corporate applications or corporate desktops from any device.  
Data remains stored remotely in the corporate data center or elsewhere.  
This type service can be provided in the office or made available at home.  
Proxied services can accommodate device interaction such as touch and gesture, but being at a remote location can introduce delays in application responsiveness. |
| Public | Access to social networks such as Facebook, Twitter, LinkedIn; personal cloud services such as email, content sharing, and personal blog.  
Access to Internet-facing applications. |
4 References
This paper refers to the following sources.

  - www.iso.org/iso/catalogue_detail?csnumber=42103
- NIST SP800-53r3. Recommended Security Controls for Federal Information Systems and Organizations

5 Resources
The following resources provide additional information that might be of interest to the reader.

- “Implications of ITIL upon IT organizations in the context of Cloud computing initiatives,” Brian Seitz,
  - http://eslibrary/ (accessible through the author)
- “Business impact of identity and privacy for the enterprise,” Bryan McMillan
  - http://eslibrary/ (accessible through the author)