



Mobility In Financial Services

A Regulatory Compliance Checklist

A Checklist Towards Regulatory Compliance

Like business leaders in every industry, decision makers in Financial Services (FS) organizations are increasingly turning to mobility to deliver on strategic objectives. They understand that mobilizing business processes can help improve customer satisfaction and response times; boost employee productivity; increase competitive advantage, and much more.

Most CIOs in these industries want nothing more than to help their line-of-business colleagues uncover new opportunities for growth.

But there's a complication: regulatory compliance. For organizations – including those in healthcare, government and indeed, finance – that face extra scrutiny from governing bodies, each new digital tool adds another layer of complexity.

Recognizing that mobile devices are increasingly powerful computing and communication tools (and that they therefore present a larger risk than ever before), regulating bodies in all regions have been hard at work to create new, relevant policies to dictate how information must be managed, stored and protected.

CIOs understand the risks of failing to comply, which go well beyond the financial impacts of audits, lawsuits and fines, although these can be significant. Harder to measure: the cost to the brand and its hard-earned reputation when customers and partners learn about breaches. Financial services companies rely on trust to build business. When that foundation begins to crack, even monoliths can fall.

Multiple Challenges for Financial Services Organizations

Even outside the industry itself, finance-related security issues make international headlines.

Corporate Networks Under Attack¹

Source: Verizon Data Breach Investigations Report

- 71% of breaches targeted user devices
- 78% of intrusions rated as low difficulty
- 54% of breaches compromised servers
- 66% of breaches go undetected for 6 months or longer

This is one of the reasons large enterprises in financial services often have entire departments devoted to compliance issues. In concert with the legal department, these specialists keep up to speed on the guidance issued by regulators wherever the company does business.

Based on how these teams interpret the 'rules' (and there's often an incredible variance in interpretation from one firm to the next), they provide recommendations to IT, whose job it then becomes to choose and implement the appropriate policies, controls and security. These rules and regulations apply to most communications between the company and its clients, between employees (internal exchanges), and between the company and its suppliers and partners.

Adding to the challenge: for multinational companies, and even for smaller companies with clients in more than one country, multiple sets of regulations apply. FINRA stipulations in the US may bear little resemblance to FCA requirements in the UK.

The High Costs of Non-Compliance

The UK's Financial Services Authority hit Credit Suisse and two other major financial services firms with fines totalling £4.2 million for failing to provide the regulator with transactional data in a timely fashion. "Without quality data we cannot properly detect and investigate market abuse, identify market-wide risks or have a comprehensive understanding of the activities of each firm," explained the FSA's director of markets, Alexander Justham. "This data is vital in our efforts to combat financial crime and we will continue to pursue firms that fail to provide quality data."²

Here Are Just a Few of the Key Regulators and Their Areas of Interest

In the United Kingdom

The Financial Conduct Authority (FCA), formerly the Financial Services Authority (FSA)

In 2009, the FSA enacted new rules requiring financial institutions to record all 'relevant' communications on employees' mobile devices. However, warnings from the industry that the technology to support these regulations was not advanced enough caused the FSA to postpone introducing the rules until November 2011. According to a March 2014 article in International Financing Review, "Analysts have estimated that since then as few as 33% of firms are in compliance. Large banks and those with operations in a number of jurisdictions are understood to be the ones having most difficulty recording staff conversations."³

In the United States

The Financial Industry Regulatory Authority (FINRA)

FINRA is the largest independent securities regulator in the US. Its rules around 'electronic communications' affect the way mobile device communications records are managed and retained, the way data on devices is encrypted, the way bring-your-own (BYO) devices access and store company data and more. For FINRA's purposes, 'electronic communications' can include instant messages, text messages, email, and posts to forums and social media sites.

United States Securities and Exchange Commission (SEC)

The SEC requires that companies produce and store records of all communications (emails, texts, instant messages, etc.) for a minimum of 3 years. Any individual or company trading stocks, bonds and other financial instruments is bound by these regulations, and violators have been fined large amounts (sometimes millions of dollars).

Gramm-Leach-Bliley Act (GLBA) Financial Services Modernization Act

To guard against the unlawful disclosure of personal financial information, the GLBA act puts in place various rules for a broad range of financial services institutions. Customer records and information must remain confidential and be securely stored, with strong physical and electronic access controls in place. All communication through emails must be kept secure and encrypted. The GLBA protects consumers' rights with regard to personal financial information and violations of the act can result in significant fines of up to \$1,000,000 plus possible jail time.

In the European Union

Markets in Financial Instruments Directive (MiFID)

The MiFID is a European Union law that provides harmonized regulation for investment services across the 31 member states of the European Economic Area (the 28 Member States of the European Union plus Iceland, Norway and Liechtenstein). The main objectives of the Directive are to increase competition and consumer protection in investment services. It requires that all electronic communications relating to securities orders be recorded and retained for a minimum of three years. Under these directives, 'electronic communications' include faxes, emails, text messages, video conferencing, B2B communication devices, instant messaging, chat room correspondence, and any 'future method of electronic correspondence'.

What to Include in Your RFP/RFQ to UEM Vendors

If you work for a financial services organization and you're part of a team evaluating Unified Endpoint Management (UEM) solutions, you need to know that the solution you choose will:

- Allow you to mobilize apps, processes and people in a way that helps you deliver on all your business goals
- Give you the flexibility to meet your compliance requirements, anywhere and everywhere, even as those needs change over time
- Support and integrate with additional mobility services that your organization may require – if not today, in the near future

Chances are, you're developing a detailed RFQ (Request for Quotation) or RFP (Request for Proposal) document that asks each vendor to address very specific questions on a host of topics, many of which will relate to compliance and to security in general.

Assembling this document can cost a lot in terms of time and resources. If you haven't done it yet, here's a sample of the kind of detail you'll want to include. This list is based on real questions that leading financial services organizations have included in their RFPs/RFQs. Although it is not exhaustive, it will give you an idea of the type of questions you should ask UEM vendors during your vetting process to determine whether their platform can help you address the relevant regulatory, privacy and security requirements.

Because it's focused on compliance-related topics, this list does not cover other important UEM factors that should be part of your RFP – for example, questions related to implementation, integration with other enterprise mobility services, tech support, devices supported, etc. For support in assembling a full RFP or RFQ, reach out to your BlackBerry® contact, who will be happy to help.

Choosing the right UEM solution means ticking hundreds of boxes. But there are some broad must-haves that make good business sense for every financial services company, regardless of size or location.

Data Leakage Prevention (DLP)

Q: How does the UEM solution separate work and personal applications and app data?

Q: How does the UEM solution ensure that data can't be 'leaked' between secure enterprise applications and personal applications?

Q: Does the UEM solution allow us to restrict clipboard copy and paste operations? Can we ensure copy and paste happens only between protected and authorized mobile apps?

Q: Does the UEM solution allow us to prevent mobile app data from being copied during device or cloud backups?

Q: Does the UEM solution provide a way to control/ restrict the transfer of data from a mobile device to a desktop/laptop when connected or tethered?

Q: Does the UEM solution allow us to disable the screen-shot feature on a mobile device? Does this differ by operating system?

Encryption

Q: Does the UEM solution provide encryption for both data at rest and data in transit? If yes, what type of encryption?

Q: What level of encryption does the UEM solution provide to separate work application and personal application data on a mobile device?

Q: Does the UEM solution enable FIPS 140-2-compliant cryptography? If yes, does it provide Level 1 or higher?

Q: Are encryption keys, initialization vectors (IV), and static salts randomly generated?

Q: Can the UEM solution be used to manage encrypted Enterprise Instant Messaging (EIM) services? To what extent?

User Privacy

Q: Can a device be remotely locked if we suspect it has been lost or left in an unsecure location?

Q: Can all data on a mobile device be wiped if it is lost or stolen? Does the UEM solution have the ability to selectively wipe only work data from the device, leaving the personal information intact?

Q: Does the use of location tracking functionality require explicit opt-in from the end user?

Q: Does the UEM solution verify a user's identity prior to resetting a password to prevent both unauthorized access to personal information and hacking attempts via social engineering?

Q: Can the UEM solution be configured to allow a device to automatically wipe itself after a certain number of incorrect authentication attempts?

Access to Cloud-Based Services

Q: Does the UEM solution allow us to restrict document and file sharing via iTunes (iOS)?

Q: Does the UEM solution allow us to restrict iCloud and other cloud services for document and file sharing?

Q: Does the UEM solution support Microsoft® Office 365™ users?

Identification and Registration

Q: Does the UEM solution offer self-service options for all employees? What features are available?

Q: Does the UEM solution operate in real time (so that users can be added or deleted immediately)?

Q: Does the UEM solution have the ability to track and restrict authorization and authentication for multiple logins on the same device (if the device is authenticated only for a set of predetermined/pre-identified users)?

Q: Does the UEM solution integrate with enterprise solutions for Identity & Access Management (IAM), and in particular, for cloud-based IDs? To what extent?

Mobile Applications Security

Q: Can we prevent user groups from installing certain mobile apps, and make other apps mandatory for particular groups?

Q: Does the UEM solution store credentials and configurations in encrypted form independent of the device?

Q: For sufficient post-event auditing: can all device and environmental attributes, including GPS coordinates, be exposed to applications and logging?

Q: Can we prevent mobile applications from trusting any client-side authentication of authorization tokens?

Q: Does the UEM solution have control over links within email, with the ability to force links to open in a secure native browser where required?

Q: Does the UEM solution enable users to open an attachment, update documents using secure editors, and send without leaving the secure container architecture?

Q: Can we use the UEM solution to set content download restrictions (e.g. for roaming)?

Q: Can we enable granular app controls to blacklist undesired apps and control VPN access per app?

Software and Policy Updates

Q: Does the UEM solution have the ability to auto- update applications remotely?

Q: Does the UEM solution allow us to enforce a check for policy and app updates as often as we choose?

Q: Does the UEM solution allow us to force an upgrade to a new mobile app version after a configurable amount of time has elapsed?

Q: Does the UEM solution provide the ability to maintain an audit trail of all updates (e.g. OS, app installation, app versions) to a device?

Q: Does the Enterprise App Store notify users about available updates?

Certificates

Q: Does the UEM solution have the capability to deploy a certificate, as well as a provisioning profile, for each application deployed to an end user?

Q: Are all digital certificates kept current, issued by a well-known certificate authority, and associated with the correct hostname?

Q: Are encryption keys protected during transit and in storage? Is access to encryption keys restricted to authorized personnel?

Containerization

Q: Can the UEM solution enable a full container mode for work apps and data?

Q: In corporate-liable scenarios, does the administrator (optionally) have full control over all applications on the device, including corporate and public applications, whether they're made optional or mandatory?

Q: Can the UEM solution restrict document and file sharing between mobile apps on the same device?

Q: What methods of authentication are provided to enable container authentication?

Q: Is the solution able to leverage those authentication types across apps? How so?

Reporting

Q: Does the UEM solution allow us to log and report on configuration, deployment, use and the availability of business data/applications on devices? Is this information made available via Microsoft® Excel® or other formats that can be manipulated?

Q: Can all mobile device data traffic be captured, including chat (IM), texting (SMS) email and phone numbers (dialed and received)?

Q: Does the UEM solution produce sufficient logs and/audit trails to support the investigation and forensic analysis of security incidents?

Network Management and Security Event Logging

Q: Does the UEM solution have the capability to log various mobility network data and voice traffic, such as PIN, SMS, phone, and BBM messages (chats, video calls)?

Q: Can all IT commands and application deployments/wipes be logged?

Q: Describe what the UEM solution requires from an external-facing firewall/security perspective.

Q: Does the UEM solution fully support Active Directory (AD)? Can configurations be assigned to users via AD groups?

Q: Do all log entries include the following attributes?:

- The time and date of the event
- The application associated with the event
- The user or process initiating the event and, if applicable, the subject acted upon
- The remote IP address of the initiating user or process
- Success or failure indication
- A detailed description of the event

Q: Can the UEM solution enforce policies based on the geographic location of the device?

Q: Does the UEM solution enable advanced gatekeeping to control access to Microsoft® Exchange ActiveSync by device?

Q: How many ports are required? (Single outbound port consolidation simplifies IT management while reducing the threat posed by malicious attacks)

Q: Can the UEM solution allow us to route all traffic through the corporate infrastructure?

Q: Please describe the UEM solution's system health diagnostics capabilities in detail.

Mobile Device Usage Policies

Q: How does the UEM solution maintain device usage policies that are applied to a profile on the device?

Q: Does the UEM solution have the ability to push updated policies to a profile on the device?

Q: Can the UEM solution validate that updated policies have been applied?

Q: Can the UEM solution be used to set user profiles for activation, SSO and proxy settings?

Q: Can it be used to limit the number and type of devices, and easily manage multiple devices per user?

Q: Can we set policy and device controls based on device ownership model (COPE, BYOD etc.)?

Passwords

Q: Can the UEM solution force users to change their passwords upon first login with an initial password or a reset password?

Q: Does the UEM solution encrypt authentication credentials in transmission and in storage?

Q: Can the UEM solution force password changes, force the use of multiple character types in password creation, and restrict the use of previous passwords? Does it allow us to restrict device use and/or wipe data after a set number of unsuccessful login attempts, and lock the device after a set time of non-use?

Q: Where are the user IDs and passwords stored for validating user credentials? How are they protected (i.e. encrypted or hashed)? If a password is hashed, is a user-specific salt used?

Mixed Security Requirements

Q: Does the UEM solution easily support all device ownership and management models such as bring your own device (BYOD), corporate-owned, personally enabled (COPE), corporate-owned, business only (COBO), choose your own device (CYOD), etc.?

Q: Does the UEM solution allow a mix of security and access policies for roles with varying sensitivities and security requirements? (e.g. employees/ partners/contractors)

Q: Does the UEM solution allow for differing policies and user capabilities based on groups or departments?

Jailbreaking/Rooting

Q: Can the UEM solution detect jailbreaking/rooting on iOS and Android™ devices? Can it be configured to take various actions including wiping the work container or the entire device when the device is out of compliance?

Q: Does the UEM solution detect when a user tries to tamper with client components, jailbreak or root the device, or uninstall clients/profiles?

Q: Can access to enterprise systems be limited/ denied based on the device's operating system version (including whether the device has been rooted/jailbroken) or its mobile device management software client version (if applicable)?

Compliance remains a constant challenge for financial services firms as their mobile ecosystem broadens and employees expect to work from anywhere as if they were sitting at their desk in the office.

¹ Available at: <http://www.verizonenterprise.com/DBIR/>

² Available at: <http://www.information-age.com/technology/information-management/1246628/credit-suisse-fined-%C2%A3175m-for-data-compliance-failure#sthash.K41JtzEm.dpuf>

³ Available at: <http://uk.reuters.com/article/2014/03/17/uk-britain-banks-phones-ifr-idUKBRE2G0VH20140317>

How BlackBerry Ticks All the Boxes for Financial Organizations

BlackBerry® Unified Endpoint Manager (UEM) provides the control and visibility IT needs with the flexibility to support all your endpoints, ownership models and use cases.

BlackBerry UEM is a part of the BlackBerry Enterprise Mobility Suite, offering a trusted end-to-end approach to security, and allowing organizations to support a wide range of endpoints, including iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry®.

BlackBerry security is trusted by thousands of enterprises around the world to lock down mission-critical data. With 70+ security certifications, more than any other mobile vendor, BlackBerry meets compliance requirements for organizations in even the most strictly regulated industries.

BlackBerry UEM provides a secure, end-to-end, behind-the-firewall outbound-initiated connection integrated into the device workspace. VPN- less secure connectivity can be set for the whole device, container or specific apps, which require access to behind the firewall resources. With BlackBerry UEM, your mobile traffic travels over the secure BlackBerry network to ensure data security, protecting your most important asset—your business data.

Choose a Solution That Grows with Your Needs

As your mobile needs evolve, BlackBerry UEM can grow with them. From secure mobile collaboration to mobile content to a wide range of secure mobile apps, BlackBerry UEM and the BlackBerry Enterprise Mobility Suite ensure you can deploy additional mobile capabilities as you need them without time-consuming and costly rip-and-replace migrations.

Choosing a single solution for your endpoint management requirements can help your organization standardize infrastructure, reduce complexity and increase ROI. Both deployment options for BlackBerry UEM—cloud and on-premise—are cost-effective and flexible so that you can scale up or down as your needs change. User-based licensing enables management of many endpoints, on any platform and with any ownership model.

Talk to us to find out how BlackBerry can address every one of the issues on this checklist.

In the meantime, visit blackberry.com/suite to learn more about our mobility management solutions, and get started with a free trial of the BlackBerry Enterprise Mobility Suite that's right for your organization.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com