

IBM IT Economics and Research

Z Security Assessment Workshop



What are you waiting for?

New Year. New Security Plan. **Now is the time.**

You are already running the premier platform to shelter your sensitive data. The next step is to put the powerful IBM Z encryption capability to work to attain a level of security far beyond what your compliance audits require. Throughout this workshop, you will have the opportunity to assess your current level of security and compare to best practices in the industry. Focus will be in the areas of *the economics of securing data, regulatory compliance and implementation.*

- ½ Day Interactive Workshop
- Geared towards clients running IBM z12 and z13
- Focused on the decision-makers and decision-influencers, in corporate security, auditing and compliance, and IT and IBM Z roles.
- Self-assessment process to identify security exposures versus best practices
- Recognize barriers to security adoption and learn how to overcome them with Pervasive Encryption
- Leave the workshop with an innovative approach to secure your data!

If you would like to schedule a session, please send an email to Sally Touscany at it.economics@us.ibm.com

IBM Z Data Security Assessment Workshop

Agenda – ½ Day Session

Topic	Description
The Cost of Security - Beware of false economies	There have been over 9.7 billion data records lost or stolen since 2013, and in only 4% of those cases was the data encrypted and therefore secure. At \$148 per record stolen, that's an astounding cost in money alone, not to mention lost customers and reputation. So, this begs the question: How secure is your data? Many businesses use physical security, or add a minimal level of encryption for some of their data, but this is likely to not be sufficient as regulations like GDPR go into effect. Instead, the new paradigm is to encrypt all the data all the time, at rest and in flight. Businesses may have hesitated to adopt this approach in the past because encryption does come at a cost. But today's IBM z14 platform has powerful advanced technology which has drastically lowered the cost, making z14 pervasive encryption not just worth the investment, but a must-have.
Compliance vs. Coverage - Just passing audits may not be enough	With pervasive encryption, IBM z14 customers have the opportunity to implement more than a minimum level of encryption needed for audits. For example, z14 data set encryption enables the data to be separated from the data set for access purposes, giving a business finer granularity when it comes to separation of powers. Bulk encryption of the data sets means that audits run faster and smoother. Likewise, insuring the data is encrypted in flight removes vulnerabilities that may be overlooked by audits, and delivers a deeper level of security demanded by today's regulations.
Implementing Pervasive Encryption - Maximizing effectiveness while minimizing disruption	Choice of approach can affect time-to-market, application quality, SLAs, etc. Disruption can lead to lost business. We will demonstrate how Pervasive Encryption is the best way to minimize disruption during development and on an ongoing basis.
Broadening the Scope - Securing data in all its uses	Today's mainframe is at an inflection point. It's moved from being a supporting platform to being a source of revenue and growth, delivering 300%+ ROI over 5 years. It's become an integral part of any businesses move to digital transformation. Connecting IBM Z to cloud computing must be done in a way that preserves data security, for example, via use of IBM Cloud Private running on Z. Similarly, considerations must be made for moving data within the data center. Because IBM Z is one of the most securable platforms, strong consideration should be made to moving new workloads to the platform (e.g., Linux workloads).