MENGAMANKAN INFORMASI SELEKSI KREDITOR SWASTA ASING UNTUK PENGELOLAAN UTANG YANG HANDAL DAN MENCEGAH KERUGIAN NEGARA

Raditya Hendra Pratama
Politeknik Keuangan Negara STAN
h3ndra@pknstan.ac.id

Abstract

Selection of Foreign Private Creditors is one of the instruments that become part of debt management of the Government of Indonesia. This selection is aimed at finding the lender with the most favorable cost offer for the Government of Indonesia. In the process communication with prospective creditors (non-resident) is often done by using email and contains important information that is very confidential in order to keep the selection process remains fair and competitive. Information Rights Management (IRM) can be applied in debt accounting information systems to provide services that allow information owners to manage who can read the information they have and what can be done about the information and when it can be done. This is part of the information security aspect consisting of confidentiality and integrity, but has not guaranteed the availability aspect. IRM can provide protection against information that is distributed at a constant level of security wherever the information is distributed. If protection has been more focused on security at the network level and less concerned about whether those with access to the network also have action authority over distributed information so that the possibility of information leakage remains a threatening issue, the IRM is a solution that can provide control to the distribution of information so that confidential information remains in-house information and retains high integrity. IRM can be used on email or on documents created using Microsoft Office programs such as.

***Keyword** : Accounting, information, control, security, debt*

Abstrak

Seleksi Kreditor Swasta Asing merupakan salah satu instrumen yang menjadi bagian dari pengelolaan utang Pemerintah Indonesia. Seleksi ini bertujuan mendapatkan pemberi pinjaman dengan tawaran biaya yang paling menguntungkan bagi Pemerintah Indonesia. Dalam prosesnya komunikasi dengan para calon kreditor (non-resident) seringkali dilakukan dengan menggunakan email dan berisi informasi-informasi penting yang bersifat sangat rahasia demi menjaga agar proses seleksi tetap adil dan kompetitif. Information Rights Management (IRM) dapat diterapkan dalam sistem informasi akuntansi utang untuk memberikan layanan yang memungkinkan pemilik informasi mengatur siapa yang dapat membaca informasi yang mereka miliki dan apa yang dapat dilakukan terhadap informasi tersebut serta kapan hal tersebut dapat dilakukan. Hal ini merupakan sebagian dari aspek information security yang terdiri dari confidentiality dan integrity, namun belum menjamin aspek availability. IRM dapat memberikan proteksi terhadap informasi yang didistribusikan pada level keamanan yang konstan ke manapun informasi tersebut didistribusikan. Jika selama ini proteksi lebih terfokus pada keamanan di level jaringan dan tidak terlalu memperhatikan apakah mereka yang memiliki akses dalam jaringan juga memiliki otoritas tindakan terhadap informasi yang terdistribusi sehingga kemungkinan terjadinya kebocoran informasi tetap saja menjadi masalah yang mengancam, maka IRM merupakan solusi yang dapat memberikan kontrol terhadap distribusi informasi sehingga informasi yang bersifat rahasia tetap menjadi in-house information dan tetap memiliki integritas yang tinggi. IRM dapat digunakan pada email atau pada dokumen yang dibuat dengan menggunakan program Microsoft Office seperti MS. Word, MS. Excel, dan MS. PowerPoint.

Kata kunci:
Akuntansi, informasi, pengendalian, keamanan, utang

ISSN : 977 25993430 04

1. PENDAHULUAN

1.1 Latar Belakang

Seleksi Kreditor Swasta Asing (KSA) dilakukan untuk memenuhi pembiayaan defisit Pemerintah Indoensia khususnya terkait kontrak pengadaan barang yang tidak mendapatkan sumber pembiayaan yang murah sehingga perlu dicari dengan mengundang calon kreditor komersial.

Dalam rangkaian proses Seleksi KSA terdapat beberapa tahapan yang harus dilakukan dan masing-masing tahapan tersebut menghasilkan informasi-informasi spesifik yang penting dan bersifat rahasia. Informasi-informasi penting tersebut dikirimkan melalui email dan memiliki fungsi spesifik sebagai berikut:

i. *Request for Interest* (RfI), merupakan dokumen yang dikirimkan kepada beberapa calon kreditor yang telah ditetapkan dalam sebuah *short-list* sehingga bersifat spesifik dan tidak boleh diteruskan atau diinformasikan kepada pihak lain yang tidak termasuk sebagai bagian dalam keputusan penetapan *short-list*. Dokumen ini nantinya akan menghasilkan jawaban berupa kesediaan atau tidak dari calon kreditor untuk mengikuti seleksi.
ii. *Request for Proposal* (RfP), merupakan dokumen yang disampaikan kepada calon kreditor yang menyatakan kesediaannya untuk disertakan dalam proses seleksi dan berisi permintaan tawaran finansial yang spesifik dan kompetitif untuk diseleksi dengan tawaran-tawaran dari calon kreditor yang lainnya. Dalam dokumen RfP ini disertakan juga dokumen *Terms of Reference* (ToR) yang berisi keterangan-keterangan resmi dari panitia seleksi terkait spesifikasi material kontrak yang akan dibiayai serta detail kebutuhan pembiayaan yang diperlukan.
iii. *Loan/Financing Proposal* (L/FP), merupakan dokumen yang berisi tawaran pembiayaan dari masing-masing calon kreditor sesuai dengan dokumen RfP dan ToR yang disampaikan oleh panitia seleksi. Dokumen ini berisi tawaran pembiayaan yang nantinya akan diseleksi dalam evaluasi sehingga bersifat sangat rahasia demi menjaga agar proses seleksi tetap bersifat adil dan kompetitif, serta tidak ada kecurangan yang dapat merugikan Pemerintah Indonesia maupun calon kreditor peserta Seleksi KSA.

Kebocoran informasi yang bersifat sensitif/rahasia dapat sangat merugikan bagi suatu organisasi serta memberikan dampak yang luas pada aspek bisnis, kepegawaian, pelanggan, dan rekanan (Lieberman, 2009). Oleh karena itu suatu organisasi harus melindungi diri dari terjadinya kebocoran informasi baik yang memiliki unsur kesengajaan ataupun yang bersifat kelalaian dari penerima informasi.

Menurut Lieberman (2009) sebagai hasil atau konsekuensi dari bocornya informasi penting dapat berupa beberapa hal merugikan bagi organisasi seperti berikut:

i. Kerugian secara finansial.
ii. Depresiasi/rusaknya kredibilitas dan nama baik di mata pelanggan ataupun rekanan.
iii. Kehilangan kesempatan bersaing dengan kompetitor.

1.2 Tujuan Penulisan

Tujuan penelitian ini adalah untuk mengetahui bagaimana IRM dapat digunakan untuk mengamankan informasi dalam Seleksi KSA untuk mencegah kerugian negara, termasuk keterbatasan IRM yang masih perlu tindakan lanjutan.

2. KERANGKA TEORI

2.1. Sistem Informasi Akuntansi

Menurut Romney dan Steinbart (2014) sistem adalah serangkaian dua atau lebih komponen yang saling terkait dan berinteraksi satu sama lain. Suatu sistem diciptakan untuk mencapai tujuan. Sistem ini terdiri dari subsistem yang lebih kecil untuk mendukung sistem yang lebih besar. Semakin besar suatu organisasi, semakin kompleks pula sistem yang digunakan. Pengertian akuntansi menurut Romney dan Steinbart (2014) adalah data yang telat diolah dan diproses. Informasi berfungsi untuk memberikan arti dalam hal proses pengambilan keputusan. Sebuah organisasi membutuhkan informasi untuk membuat keputusan yang efektif. Akuntansi adalah suatu proses mengidentifikasi, mengumpulkan, mencatat, menyimpan dan mengolah data.

Dari pengertian-pengertian di atas, dapat disimpulkan pengertian sistem informasi akuntansi.Terdapat beberapa ahli yang telah mengemukakan pendapatnya mengenai pengertian sistem informasi akuntansi. Romney dan Steinbart berpendapat bahwa sistem informasi akuntansi adalah suatu sistem yang terdiri dari kegiatan mengumpulkan, mencatat, menyimpan dan mengolah data untuk menghasilkan informasi bagi pengambil keputusan. Unsur dari sistem ini meliputi orang, prosedur dan instruksi, data, perangkat lunak, instruktur teknologi informasi, serta pengendalian internal dan ukuran keamanan.

2.2 Deskripsi IRM

Menurut Pemerintah Queensland (2008) Information Rights Management (IRM) adalah komponen/feature yang disediakan untuk memberikan layanan berupa kemungkinan bagi penulis dokumen untuk mengatur siapa yang dapat membaca dokumen mereka dan apa yang dapat dilakukan terhadap dokumen tersebut serta kapan hal tersebut dapat dilakukan.

Tanpa IRM, dokumen elektronik yang beredar tidak dapat dikontrol dan dapat dicetak, disalin, dan diteruskan secara bebas kepada siapa pun. Pengiriman informasi melalui email dan melewati jaringan yang aman dapat melindungi informasi pada area transit (tujuan) dokumen tersebut, tetapi tidak memberikan kontrol atas apa yang dilakukan oleh penerima dokumen terhadap informasi tersebut.

Menurut Pemerintah Queensland (2008) IRM dapat digunakan untuk mencegah pencetakan atau penyampaian informasi dalam email dan untuk membuat informasi tersebut tidak dapat diakses oleh penerima setelah tanggal kedaluwarsa yang telah ditetapkan. IRM mampu membuat oleh orang lain selain dari penerima yang ditentukan tidak dapat membaca dokumen yang berisi informasi tersebut.

2.3 Peran Penting IRM

Menurut Lieberman (2009) IRM dapat membantu suatu organisasi untuk memenuhi dua kebutuhan fundamental berikut:

ISSN : 977 25993430 04

i. Membatasi akses untuk informasi yang bersifat sensitif/terbatas/rahasia.

ii. Memberikan kontrol terhadap informasi yang bersifat rahasia sekaligus memberikan nilai terhadap integritas informasi tersebut.

Menurut Yang Yu dari Stony Brook University, organisasi yang ada pada saat ini mulai serius dalam menerapkan keamanan informasi dalam jaringan organisasi mereka. Kebanyakan organisasi sudah mulai menggunakan sistem keamanan seperti *firewall, log-in security*, dan teknologi lainnya untuk melindungi properti/aset intelektual organisasi. Namun demikian, perlu disadari bahwa teknologi keamanan jaringan tersebut memberikan batas keamanan dari pihak luar yang tidak dikehendaki untuk melakukan akses kepada informasi dalam jaringan organisasi tetapi tidak membatasi aktor-aktor dalam organisasi untuk melakukan apa saja terhadap informasi yang mereka peroleh termasuk membocorkan informasi tersebut kepada pihak-pihak yang tidak berwenang atau bahkan dilarang memperoleh informasi tersebut (Infosys Limited, 2010).

Dengan keadaan tersebut di atas, maka kemudian disadari bahwa keamanan tidak hanya perlu dibangun dalam jaringan organisasi tetapi juga dalam informasi yang menjadi aset organisasi agar tetap menjadi *in-house information* dan tidak menyebar ke pihak-pihak yang tidak berwenang dan tidak berkepentingan.

Menurut Yang Yu dari Stony Brook University IRM dinilai dapat memberikan solusi cepat untuk menjaga informasi rahasia dari akses dan penyalahgunaan pihak-pihak yang tidak berwenang baik dari dalam maupun luar organisasi. IRM dapat meminimalisasi potensi penyalahgunaan informasi melalui mekanisme *forwarding, copying,* dan pencetakan informasi tersebut dalam bentuk fisik. Hal tersebut dilakukan dengan menonaktifkan fungsi-fungsi tersebut sehingga tidak dapat dilakukan kecuali dengan izin dari pemilik yang mengirimkan informasi tersebut.

3. METODE PENELITIAN

Metode yang digunakan untuk memperoleh data terdiri dari dua metode, yaitu:

1. Metode studi literatur, yaitu dengan membaca sejumlah buku, artikel dan sumber lain untuk memperoleh data teoritis serta pemahaman mengenai permasalahan dalam penelitian ini.
2. Metode studi lapangan:
   a. *Focus Group Discussion*
      Metode ini dilakukan dengan cara melakukan diskusi dengan pihak-pihak yang berhubungan dengan proses seleksi KSA di Kementerian Keuangan.
   b. Observasi
      Penulis melakukan pengumpulan dokumen-dokumen terkait seleksi KSA dengan mengunjungi objek secara langsung dan melakukan studi langsung di lapangan bagaimana sistem dilaksanakan.

4. HASIL PENELITIAN

4.1 Skenario Proteksi Yang Diberikan IRM

Terdapat beberapa cara yang sudah lebih familier untuk digunakan dalam mengatasi kebocoran informasi yang biasanya membatasi akses kepada jalur-jalur data dan

ISSN : 977 25993430 04

informasi dalam jaringan komunikasi organisasi, namun biasanya tidak memberikan proteksi yang terkait dengan informasi itu sendiri.

Proteksi menggunakan IRM dapat dilakukan pada dua aspek, yang pertama adalah melakukan proteksipada dokumen informasi yang dikirimkan sebagai lampiran/*attachment* yaitu dengan mengaktifkan IRM pada dokumen-dokumen MS. Office yang berisi informasi rahasia/terbatas, sedangkan yang berikutnya adalah pada aspek email itu sendiri dengan mengaktifkan IRM pada Microsoft Outlook (Turick, 2003).

Dalam skala kecil IRM dapat juga digunakan oleh individu untuk melakukan proteksi terhadap informasi-informasi pribadi yang tidak ingin tersebar luas ketika dilakukan pengiriman informasi tersebut, sedangkan dalam skala yang lebih luas IRM dapat membantu sebuah organisasi untuk mengelola dan menerapkan kebijakan yang terkait dengan perlindungan aset/properti intelektual organisasi, sehingga dalam proses distribusi informasi tersebut kepada pihak-pihak yang berkepentingan tetap memiliki kontrol yang melindungi kepemilikan dari informasi tersebut. Menurut Microsoft Corporation (2011) ada beberapa hal yang dapat dilakukan oleh IRM dalam upaya memberi proteksi terhadap distribusi informasi, yaitu:

i. Membantu mencegah penerima informasi yang tidak memiliki wewenang untuk melakukan penerusan, penggandaan, modifikasi, pencetakan, dan mencuplik informasi yang didistribusikan.
ii. Mencegah terjadinya penyalahgunaan /pencurian informasi dengan cara digandakan menggunakan fungsi print-screen yang ada pada Windows
iii. Memberikan proteksi pada level yang sama ke manapun informasi tersebut terdistribusi atau disebut "*persistence protection*".
iv. Memberikan proteksi yang konstan untuk informasi yang dikirim melalui lampiran/*attachment* email selama informasi tersebut dibuat dalam format yang ada pada program MS. Office seperti Word dan Excel.
v. Membantu melindungi informasi pada email atau dokumen yang dilampirkan dengan menerapkan batas waktu kadaluwarsa, sehingga informasi yang didistribusikan tidak lagi dapat dibaca setelah periode waktu tertentu.
vi. Membantu penerapan kebijakan organisasi dalam mengelola penggunaan dan pendistribusian informasi di dalam dan di luar organisasi.

Selain hal-hal yang dapat dilakukan dengan menggunakan IRM sebagaimana tersebut di atas, terdapat juga beberapa hal yang tidak dapat dilakukan oleh IRM dalam usaha proteksi informasi sehingga perlu dilakukan antisipasi lanjutan seperti melindungi informasi yang dikirimkan kepada penerima pesan untuk tidak terhapus, dicuri, dibajak dan ditransmisikan oleh program-program yang bersifat merusak seperti *trojan horses, keystroke loggers,* dan beberapa jenis *spyware*, dan mencegah hilangnya sebagian atau keseluruhan dari informasi akibat dari operasi virus pada computer, atau *screen capturing*.

ISSN : 977 25993430 04

4.2 Dokumen Informasi Yang Dapat Diproteksi Menggunakan IRM

Menurut Microsoft Corporation (2011) proteksi dengan menggunakan IRM dapat dilakukan terhadap beberapa jenis *file*/dokumen yang dibuat dengan menggunakan program dari MS. Office. Beberapa jenis *file*/dokumen yang dapat diproteksi menggunakan IRM yaitu f*ile*/dokumen MS. Word, MS. Excel, dan MS. PowerPoint.

Jika seseorang melakukan proteksi terhadap dokumen Ms. Office, maka dokumen tersebut akan dienkripsi dan isinya akan dikodekan dalam bentuk yang tidak bisa dipahami jika dilihat apa adanya (Zhou, 2006). Selain itu program yang akan digunakan untuk membuka dokumen tersebut juga harus terlebih dahulu mengaktifkan *feature* IRM.

Perlu dicatat bahwa jika jenis *file*/dokumen tersebut di atas dilampirkan dalam e-mail yang menerapkan IRM seperti dalam pesan Microsoft Outlook misalnya, maka *file*/dokumen tersebut akan secara otomatis menerapkan juga IRM (Microsoft Corporation, 2011).

4.3 Mengaktifkan Feature IRM

Meskipun IRM adalah layanan *free service*, namun untuk mengaktifkan IRM pertama kali dibutuhkan langkah-langkah berikut:

i. Pimpinan organisasi atau pejabat yang berwenang menetapkan kebijakan terkait dengan distribusi dokumen yang bersifat rahasia berupa siapa yang dapat menerima dan membaca dokumen tersebut serta kapan dokumen tersebut dapat dibaca.
ii. Memberlakukan *Restricted Acces* dalam program Ms. Office yang digunakan untuk membuat dokumen.
iii. Setelah itu akan muncul *dialogue box* yang dapat menampilkan *user account* berupa alamat email yang dapat diatur *user account* apa yang akan digunakan untuk melakukan pengaturan terhadap kebijakan distribusi dokumen tersebut.

4.4 Menetapkan Batasan Terhadap Informasi Yang Akan Didistribusikan

Ketika IRM telah diaktifkan, maka setiap dokumen yang berisi informasi terbatas dapat diproteksi dengan menggunakan IRM setelah terlebih dahulu ditetapkan batasan distribusi informasi tersebut.

Batasan-batasan yang ditetapkan dapat berupa *user account* yang dapat membaca pesan dalam dokumen yang didistribusikan serta kapan dokumen tersebut kadaluwarsa. Sedangkan *Access Level* atau *Permission Level* yang diberikan dapat diubah dengan memilih beberapa tingkat seperti di bawah ini:

a. ***Read*** level yang memberikan *read permission* kepada *user* yang dipilih untuk dapat membaca dokumen namun tidak dapat melakukan modifikasi, pencetakan, maupun mengopi dokumen tersebut.
b. ***Change*** level yang memberikan *change permission* kepada *user* yang dipilih dan ini berarti *user* tersebut dapat membaca dokumen, melakukan modifikasi terhadap dokumen dan menyimpan perubahan tersebut namun tidak

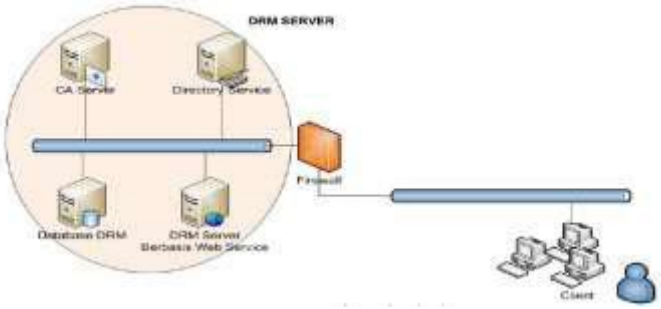
ISSN : 977 25993430 04

diberikan kewenangan untuk melakukan pencetakan dokumen.

c. ***Full Control*** level yang memberikan *full control permission* kepada *user* yang dipilih sehingga *user* tersebut memiliki wewenang untuk melakukan tindakan-tindakan sebagaimana yang dimiliki oleh pembuat dokumen.

4.5 Prinsip Kerja IRM

Setiap dokumen elektronik yang telah dibuat dan ingin memproteksi informasi didalamnya maka terhadap dokumen elektronik tersebut dapat diterapkan *Digital Rights Management* (DRM). Proses ini melibatkan enkripsi berbasis kriptografi yang mempunyai *public key* dan *private key*. Sistem yang menghasilkan *public key* dan *private key* dapat berperan sebagai *license server*.



Gambar Desain lokal pada sistem DRM

4.6 Mengaplikasikan IRM Pada Organisasi Publik

Organisasi pemerintahan sangat identik dengan dokumen rahasia dan bersifat terbatas. Namun demikian upaya pencegahan penyalahgunaan atas dokumen rahasia tersebut sepertinya belum optimal.

Berdasarkan pada pengamatan pada proses seleksi KSA, secara umum pengamanan arus informasi dalam jaringan teknologi informasi yang selama ini digunakan biasanya lebih berorientasi pada keamanan jaringan organisasi. Hal ini dapat dilihat dengan diberlakukannya *security log-on* dan penggunaan *firewall* pada jaringan dan perangkat komputer di instansi-instansi pemerintah. Hal ini sangat membantu dalam membatasi pencurian informasi oleh pihak luar seperti serangan "*man in the middle attack*", namun tidak mampu mengontrol dokumen begitu dokumen tersebut diunduh ke dalam *hard disk* local.

Secara infrastruktur tidak diperlukan investasi besar untuk menerapkan IRM dalam mengamankan informasi pada organisasi pemerintah. Namun demikian, perlu dipersiapkan beberapa hal sebelum organisasi pemerintah dapat menerapkan IRM dengan baik sebagai bagian dari kebijakan organisasi yaitu:

i. Memiliki *Data Governance and Classification Policy*. Untuk dapat menetapkan informasi yang terdapat dalam organisasi diperlukan pengelolaan dan kebijakan yang memberikan definisi dari informasi-informasi yang ada, apakah ada informasi yang bersifat rahasia/terbatas dan seperti apa pengelolaan yang ditetapkan atas informasi tersebut.

ii. Menetapkan informasi mana saja yang bersifat rahasia dan berada pada wewenang siapakah informasi tersebut, serta siapa saja yang

ISSN : 977 25993430 04

memerlukan penggunaan informasi tersebut.

iii. Menetapkan bagaimana otorisasi akan diberikan kepada setiap pegawai yang ada dalam organisasi, apakah akan menggunakan satu sistem otorisasi dan berlaku untuk semua jenis informasi, atau akan diterapkan otorisasi yang dinamis.
iv. Menetapkan standar yang jelas terkait keadaan yang diharapkan setelah menetapkan IRM sebagai bagian dari pengelolaan informasi organisasi.
v. Diperlukan pengawasan apakah penerapan teknologi IRM berpengaruh positif terhadap proses bisnis organisasi atau justru memberi dampak negatif.
vi. Menyusun mekanisme audit atas kepatuhan terhadap kebijakan organisasi dalam menetapkan batasan-batasan terhadap organisasi.

5. KESIMPULAN

Dengan uraian tersebut di atas, dapat dimengerti bahwa keamanan atas informasi tidak hanya terbatas pada keamanan jaringan sebagai tempat lalu lintas informasi tersebut. Salah satu faktor yang harus diperhatikan adalah bagaimana distribusi atas dokumen yang berisi informasi rahasia/terbatas.

IRM merupakan salah satu solusi cepat yang dapat diimplementasikan untuk mengatasi masalah penyalahgunaan informasi. Hal ini berlaku dalam skala kecil seperti individu maupun dalam skala yang besar seperti sebuah organisasi.

Kelebihan yang ada pada IRM yaitu menyediakan keamanan dari sisi dokumen informasi dapat dioptimalkan bersama dengan keamanan secara jaringan dan penyimpanan data dalam *database*. Dengan demikian, setiap informasi yang bersifat terbatas/rahasia dapat terjaga dan terkontrol baik ketika terdistribusi maupun ketikan tersimpan dalam *hard disk* lokal organisasi. Keamanan yang bersifat menyeluruh ini diharapkan dapat memenuhi keseluruhan aspek dari keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*.

Pemanfaatan IRM dalam Seleksi KSA dapat memberikan perlindungan tambahan yang memadai terhadap distribusi informasi-informasi penting yang bersifat rahasia sehingga dapat membantu proses seleksi yang adil dan kompetitif. Hal ini dikarenakan kewenangan yang ada pada masing-masing pegawai yang terlibat dalam proses seleksi dibatasi sesuai dengan otorisasi yang diberikan oleh pemilik informasi.

DAFTAR PUSTAKA (*REFERENCES*)

Danny Lieberman. *Preventing Intellectual Property Abuse, A Comparison Between Information Rights Management and Data Loss Prevention.* Creative Commons Attribution License. 2009

Hong Zhou. *Evaluation of Certificate Revocation in Microsoft Information Rights Management v1.0*. October 2006

Information *Rights Management Solution: Securing Information Exchange in Outsourcing Arrangements*, Infosys Limited, 2010

IRM User Guide, MTR, 2011

John Prathab, 2011. *Important Question to Ask Before Deploying Information Rights Management.* (Seclore)

Available at: http://blog.seclore.com

Kurniawan, A. (2010), Digital Rights Management Sebagai Solusi

ISSN : 977 25993430 04

Keamanan Dokumen Elektronik, *Jurnal Sistem Informasi MTI UI*, 4 (2), 93 -99.

Microsoft Corporation, 2011. *Information Rights Management in the 2007 Microsoft Office system*. (Microsoft Office) [online] Available at: http://office.microsoft.com

Queensland Government (2008), "*What is Microsoft Information Rights Management?* Queensland: Queensland State Archive.

Turick J. (2003). *Information Rights Management in Microsoft Office Outlook 2003*© Microsoft Corporation.

Viktor Mayer-Schönberger. Beyond Copyright: Managing Information Rights With DRM. *Denver University Law Review*, 84 (1), 181 – 198.

Yang Yu and Tzi-cker Chiueh. *Enterprise Digital Rights Management: Solutions against Information Theft by Insiders.* Computer Science Departement. Stony Brook University.