IBM and NASD Response to CESR

Mandate to CESR regarding technical advice on possible implementing measures concerning the Transparency Directive: Storage of regulated information and filing of regulated information. CALL FOR EVIDENCE.

July 2005

A European Listed Companies Information Database (ELCID)

Contents

1.1 Specific Terms of Reference

1.2 Context

1.3 The Joint Response of IBM and NASD

2.0 Why are IBM and NASD Responding

- 2.1 Credentials
- 2.2 Structure of this Document

3.0 Executive Summary

4.0 Expected Environment

5.0 Implementation Considerations

6.0 Role of Competent Authorities

Appendix

Issues on which CESR is invited to provide advice, with corresponding IBM/NASD views: drawn from section 3 of 3rd Mandate

Attention: M. Fabrice Demarigny

Secretary General
Committee of European Securities Regulators
11-13 Avenue Friedland
75008 Paris

August 31st 2005

Dear M. Demarigny,

IBM and NASD are pleased to have the opportunity to respond to the Committee of European Securities Regulators' Call for Evidence on its latest mandate "regarding technical advice on possible implementing measures concerning the Transparency Directive: Storage of regulated information and filing of regulated information" (CESR/05-493).

1.1 Specific Terms of Reference:

In the mandate the Commission asks CESR to provide:
• An opinion on two preliminary issues, how agreements of interoperability of Officially Appointed Mechanisms (OAMs) could be obtained and an analysis of cost and funding implications for Member States at the initial stages of the creation of a EU-wide network;
• Secondly, CESR shall provide advice on a number of technical issues regarding the role of the officially appointed mechanism for the central storage of central storage of information (Article 21(2)) for the Transparency Directive, in this regard CESR shall also provide technical advice on the role of the Competent Authority in supervising the OAM and provide an assessment of the costs of setting up an OAM that meet the standards.
• Thirdly, CESR shall provide technical advice on the filing of regulated information by electronic means with the competent authorities (Article 19(1)), and alignment of this procedure with that of the filing with the OAM.

This response from IBM and NASD addresses the three sections of the mandate and also makes some reference to the Progress Report on the first mandate delivered to the Commission on 30th March 2005 (CESR/05-150b) and the technical advice delivered on 30th June 2005 (CESR/05-408)

1.2 Context

This response by IBM and NASD is made in the broad context of the Lisbon Agenda, the prime driver for the whole FSAP process.

1.3 The Joint Response of IBM and NASD

IBM responded in January 2005 to the previous consultation on Section C, Progress Report on the Role of the Officially Appointed Mechanism (Article 17 1a) and the Setting up a European Electronic Network of Information about Issuers (Article 18) and Electronic Filing. In that document it set out its overall vision for a Central Storage Mechanism which it codenamed ELCID – A European Listed Companies Information Database.
Since providing that response, IBM has teamed with NASD, bringing together a knowledge of the state-of-the-art in technology with experience in the operation and regulation of markets, to develop further the architecture and concepts contained in ELCID. Driven by discussions at many levels with markets, their participants and regulators, IBM and NASD are working on a number of projects which improve the transparency and efficiency of markets while providing for effective, common-sense

regulation. Recent efforts include the critical infrastructure elements necessary for the linking of markets, whether the goal is to integrate the national markets of a region or to link competing domestic markets and trading systems. These elements include

- A flexible consolidated database of issuer information, built to accommodate the emerging XBRL and XML data standards and standards for unique business identifiers
- A consolidated tape and transactions database with integrated surveillance and analytical capability
- Combined registration depository for authorised individuals and firms

IBM and NASD have already jointly had open and productive discussions with CESR, and we wish to continue that engagement by responding to this call for evidence. We trust you find our response to be interesting, innovative and practical. We are available to discuss it with you and other industry stakeholders in order to help progress discussions and lead to a fully viable implementation.

Yours sincerely

Piet Van de Velde
Global Head Markets Infrastructure
IBM Global Financial Markets

Nick Bannister
Senior Vice President
NASD International

2. Why are IBM and NASD Responding?

There are three main reasons why IBM and NASD are responding to the CESR TOD consultation:

1. To help deliver the goals set by the Lisbon agenda, which will directly help to lower the cost of capital of all issuers.

2. To provide added value based on our combined experience of relevant technologies and regulatory requirements and processes.

3. IBM and NASD are independent – We are not direct market participants in the industry, nor are we providers of market information. We are therefore offering not only a European but also a global view, recognising that European capital markets are reliant on global capital flows to a very large extent.

2.1 Credentials

NASD

When it comes to securities regulation and its application, NASD understands what is required. Nearly 70 years of experience serving and regulating the US markets have allowed NASD to build unparalleled expertise in increasing market integrity and building investor confidence. Building on this experience and international best practice, NASD's International Department has worked with a number of markets worldwide to apply our expertise to problems they face, taking full account of local markets and conditions. Both new and established markets are turning to NASD International for practical customised solutions, and we have already helped shape regulatory environments in Europe, Southeast Asia, the Middle East and Central America.

NASD's International Department focuses on four major areas: Advisory Services, Education and Training, Regulatory Technology, and Dispute Resolution. Our clients have included major international aid organisations as well as governments, regulators and exchanges. Our projects have included a wide range of activities, including:

- Developing training programs and an operations manual for the client's regulatory policies, procedures and operations.
- Developed a roadmap for the development and implementation of a market surveillance system to monitor the client's capital markets.
- Advised a client on how to develop and operate an effective dispute resolution system.
- Advised a client on the development of a regulatory policy strategy aimed at defining and strengthening self-regulatory organization capabilities
- Designed, developed and delivered specialized training programs for market professionals and regulators

IBM

IBM is a leading global technology provider with proven practical experience of delivering complex solutions in many industries including financial markets. In particular it has developed technologies capable of handling, in one architecture, complex documents, including those which encapsulate forms of XML, together with high speed streaming data such as market ticks.

Regulators around the world, including competent authorities in European Union Member States, in the US, Japan, and other countries are increasing their oversight of the internal controls and reporting

by listed companies in producing information for their investors and potential investors. IBM has already created and delivered to customers successful solutions, which integrate enterprise data from the widest possible array of sources into a single repository, providing compliance reports and associated audit trails for the amalgamation of such data, thereby securing long term evidential data. Markets infrastructure solutions using IBM technology distribute vast quantities of regulated data to financial market users throughout the world today, deploying complex algorithms to maintain fair markets, under service level agreements. This has given IBM first hand experience of the challenges faced by issuers in regulatory reporting compliance.

2.2 Structure of this document

IBM and NASD have submitted a comprehensive response within this document. This document begins with an executive summary, an analysis of the expected environment, a discussion of the implementation issues, and a review of the role of competent authorities. The whole document is supported by an Appendix, which in tabular form details our views on each specific issue as set out in section 3 of the mandate.

3.0 Executive Summary

IBM and NASD are pleased to offer CESR our views on the implementing measures concerning the storage and filing of regulated information, taking full account of the options expressed in CESR's Progress Report and the new Mandate from the Commission. IBM and NASD are strong supporters of the overall goal of the Transparency Obligations Directive (TOD) in achieving a single market in financial services and increasing capital flows.

We support the idea that a well-informed market is an excellent 'regulator', creating a level playing field for all investors – institutional and retail. That view led us to advocate a single central storage mechanism acting both as a "one-stop-shop" for all users – retail and institutional investors and also regulators – and additionally as a pan-European utility into which all listed companies could submit their regulated information. Critical to the long-term performance and cost of such mechanism would be the adoption of an electronic format for submissions and the structuring of the data in submissions, using XML/XBRL, to facilitate the subsequent searching and manipulation of the core data by users.

We expressed the view that the most appropriate governance model for such a utility was a hybrid one, based on a "Private contractor: competent authority oversight". This ELCID utility would create, deliver and operate a single Pan European Central Storage Mechanism, the use of which for public issuers would be mandated within national competent authority requirements. The Central Storage Mechanism would be operated under licence granted by a dedicated body set up for that purpose by EU competent authorities (possibly encouraged by the public sector). We perceive the utility would be licensed as it would be providing a regulated service and licensing would be a pre-requisite of its launch.

Given the active engagements that IBM and NASD have had in implementing and operating similar regulatory systems, and after significant investment in proactively modelling an ELCID vehicle, we believe that a single utility does provide the lowest cost and most clearly transparent implementation. We note that CESR implied some concerns that IBM and NASD were underestimating the costs of delivering the objectives of TOD using the full ELCID single mechanism solution. Our continuing engagement in similar projects elsewhere in the world persuade us that our original approach can indeed deliver the necessary capabilities with exceptional price performance in line with our earlier statements to CESR.

The architecture was designed with a view to handling not only those documents specifically covered by the Transparency Obligations Directive but also other market information covered by other directives or competencies.

Nevertheless we recognised that there were political and legal obstacles to creating a single such mechanism, so allowed, within the architecture, for the co-existence of a broadly pan-European utility with a number of Member States opting for separate national utilities. We expressed the view that such a hybrid environment could still deliver the benefits of a full pan-European "one-stop-shop" for investors provided that measures were taken to ensure that information was exchanged between utilities freely and in a timely manner. With regard to the latter point, we also put forward the view that, with currently available and proven technologies, submissions could be received, retransmitted and stored for global access with close to zero latency.

On the issue of end user access we recognised that an ELCID could either operate as a direct one-stop-shop access point for end users, or act as an information hub supporting access to pan-European information through for instance local competent authorities' websites

We further offered the ELCID architecture as a model for national or multinational mechanisms, believing that common infrastructure design would allow the sharing of development costs, facilitate the transfer of information between mechanisms, and enhance the harmonisation of European capital markets.

We note that the initial conclusions of the Commission and of CESR, and the direction of the examination of implementing measures requested in the mandate do not preclude this overall approach albeit that the core of the directive will support separate national Officially Appointed Mechanisms. We particularly note that the preliminary issues on which CESR is asked to give advice include

- "a final objective of offering a one-stop-shop for end users"
- governance in "the cases where two or more Member States would decide to officially appoint a joint mechanism for the central storage of regulated information"
- this governance to recognize the long term need to manage the evolution of standards "over time in case of technical developments"
- "whether it would be desirable in order to facilitate automatic processing of the regulated information, including the time recording procedure, to require issuers to use input standards (such as XBRL, or similar formats) and templates (such as standards forms) for regulated information as a condition for the filing of information with the OAM"
    - We particularly note that CESR (Progress Report section 3) is aware of the use of electronic filing to facilitate the sharing of information
- "minimum standards in terms of timely access to the regulated information"
    - We further note CESR's recognition (Progress Report Section 1) that storage mechanisms have the potential to disseminate regulated information in close to real time, thereby enabling the storage mechanism to be the fastest route by which users may access even time critical data.

While noting these areas of common perception and future opportunity, we also realise that the initial regulatory environment is likely to assume multiple national OAMs networked together to deliver an appearance of a one-stop-shop for end users. IBM and NASD believe that large elements of the overall ELCID vision will contribute to cost effective and highly performing implementations even with this initial strategy. We also believe that there will be early acceptance by a number of member states that a shared infrastructure is the optimum solution. We set out below our detailed comments on the issues on which CESR must deliver advice, demonstrating our commitment to contribute to the success of all variants of OAMs, whether separate national, shared multinational or indeed fully pan-European.

4. Expected Environment

The Progress Report from CESR and the July Mandate itself indicate that, within a set of given standards, flexibility in the execution of the Transparency Obligations directive should be expected. The interpretation of the report and the mandate lead IBM and NASD to a number of assumptions on which this submission is based. Before making recommendations for technologies and approaches which would aid the implementation of TOD mechanisms, we will set out the environment in which we expect the storage mechanisms to operate:

Member States will each be empowered to appoint an Officially Appointed Mechanism to operate a filing and storage system for regulated information.

This OAM could be operated by the Competent Authority itself, or by a specifically appointed (commercial or public) entity.

There will be a heavy emphasis on ensuring that initial submission is secure with regard to the authenticity of origin and the non-repudiation of the filing once stored; and also with regard to the sharing of information between OAMs.

There is recognition that sharing of costs might make it desirable to allow the storage of regulated information under TOD to be combined in a number of ways

- two or more member states appointing the same OAM
- combining TOD storage with other similar information storage
    - either other listed companies information
    - or unlisted companies information
    - or commercial value-added information

With regard to access there is a preference for giving free access to retail users which exerts downward pressure on the cost of the mechanism.

There is also a clear view that users should have a one-stop-shop for all European regulated information, and that this should be on a timely basis even if that tended to equal the separate dissemination mechanisms for speed.

The one-stop-shop could be achieved by a peer-to-peer approach where all OAMs shared data with each other, or by a hub-and-spoke approach where a single pan-European central storage mechanism holds all regulated information of European listed issuers.

Whichever network solution is adopted there will be a need for common standards.

With regard to format of data there is a clear favouring of electronic submission and of the structuring of those submissions using input standards such as XBRL and templates such as X Forms.

There is also clearly a pressure to achieve early implementation which will also have to recognize that interim national storage mechanisms will in the meantime have been established.

IBM and NASD are confident that the ELCID architecture that was proposed in IBM's January submission to the previous round of consultation, has been further developed and tested; and is ready to be implemented in this new, more flexible environment.

5.0 Implementation Considerations

1 Agreement on Interoperability of OAMs

There is agreement at the ESC that the national legislators will decide on who should be appointed for the operation of the storage mechanism. This is likely to lead to a variety of technologies for implementing the national storage mechanisms; and this in turn will lead to complexity in technology and in regulatory interpretation in the exchange of regulated information between OAMs. The issues to be managed have been identified as threefold: there is the technical interoperability; there is the ongoing control and supervision; and there is agreement on costs and funding

Technical Interoperability

IBM and NASD concur with CESR in identifying two broad approaches to sharing information: either a peer-to-peer approach, or a hub-and-spoke approach.

For the peer-to-peer scenario, a publish and subscribe messaging system, where each OAM automatically publishes to its OAM peers, is an approach utilizing commonly available technologies. Care must be taken to ensure full acknowledgement of receipt from the full set of peers to coincide with general availability of the information on a simultaneous basis. This also requires that all OAMs are able to capture and republish such events with close to zero latency. Similarly all peers must be involved in testing processes before any format changes or technology changes by an individual OAM are put into production. It will be particularly important to ensure that all OAMs move concurrently to new versions of XBRL for instance. If one OAM uses a proprietary software package which falls out of synchronisation with those revisions, there would be the danger that that member state would fall out of the network or delay technical advance elsewhere.

A hub-and-spoke approach where a central storage mechanism handles the network traffic could also use a zero latency publish-and-subscribe technology to move information from one OAM to all others. There is still the problem of monitoring simultaneous availability of information on all OAMS, but the problem of managing testing can be eased – the central hub could test on behalf of all others.

There also exists a form of replication and transformation technology which a central hub could deploy: this holds rules for sensing state changes in the databases of the OAMs, automatically replicating those data items to the central store and replicating them onwards while transforming one data structure to another. This approach would also offer a level of disaster recovery and availability beyond that developed by each individual OAM, and potentially a longer term data storage facility for archived materials.

As CESR pointed out this hub could be the one-stop-shop for access by retail users and regulators thus performing the public service obligation of the OAMs; or to support with international information the websites of the national regulators which would act as that one-stop-shop.

Governance

With either technical architecture there would still be the need for monitoring and control, for resolution of disputes and allocation of fault, and also for the ongoing choice of input standards and templates. IBM and NASD believe that the appropriate approach is for the network to be subject to a Central Storage Mechanism Committee mandated by all the competent authorities and tasked with creating and monitoring the standards of operation of the pan-European network (and of the Central Storage Mechanism if a hub-and-spoke network approach were adopted). An operating board, accessing appropriate technical resources from the OAMs, would be responsible to the participating OAMs and Competent Authorities.

Such types of governance are successfully operating around the world – eg the ABA Committee on Uniform Security Identification Procedures (CUSIP), and the Continuous Linked Settlement (CLS) Bank to which IBM made reference in its previous submission.

Costs and Funding

IBM and NASD have examined through their ELCID project the likely costs of designing, implementing and operating a pan-European central storage mechanism, and have shared with the Commission and CESR those costs, recognizing the conditions that we attached to those cost statements. Remodelling the costs to project those for an individual OAM; for a multinational but not fully pan-European OAM, or for ELCID to act purely as the central hub of a hub-and-spoke network is a contribution which it is willing to make to expediting the technical advice that CESR is about to prepare.

IBM and NASD have specific successful experience of regulated information systems deployment and more general large scale repository and publish-and-subscribe mechanism operation. This background leads us to advise that there is a large fixed cost component in the design, implementation and operation of such a system, with only relatively small benefits of scale. The costs of building a single OAM with all the data capture, storage management and access management are similar to those of a pan-European system. We therefore welcome the willingness of the Commission and CESR to support multinational utilities which can support multiple member states.

An extension of this thinking would be to offer the Central Storage Mechanism for such a consortium of states as the hub of the integrated network. Well understood and commercially proven access control technologies would allow most of the design and operational benefits of a shared system while rigorously preserving data segregation for individual member states.

2 Quality Standards

2.1 Security and Certainty as to Information Source

Security is a continuously evolving field. As we explain in Section 6 we would propose a central standing committee to keep all standards, including those for security, under constant review.

However, in current circumstances we would recommend a layered approach to security based on our experience of other regulated information repositories including EDINET, SEDAR and EDGAR (IBM has recently acquired the XForms specialist PureEdge which developed the well regarded EDGARLink solution). These recommendations are obviously general and we would be very prepared to refine them as the exact environment demands.

Information Acquisition: We recommend that OAMs deploy end-to-end electronic form-based approvals with digital signature technology. Advanced approval functionality supports the validation of the signer's identity, confirmation of the certificate validity, and invalidation of signatures on documents that have been modified. XML itself has no inherent security or communications mechanisms, but, critically, is able to take advantage of outside security, including digital signatures and encryption, and to be transported using a variety of network protocols. The trend in the electronic forms software world is toward such use of XML.

The process should require an initial registration phase to establish a filer’s identity, and the issuance of a digital certificate to be used in the filing process.That process should include a confirmation stage, which would cover the initial format check and also ensure non-repudiation of the filing itself. A simplified view of such a process is given in Fig 1 below.

In the interests of clarity in the diagram, we have not attempted to include time-stamping. We will cover that issue below in the Time Recording section.

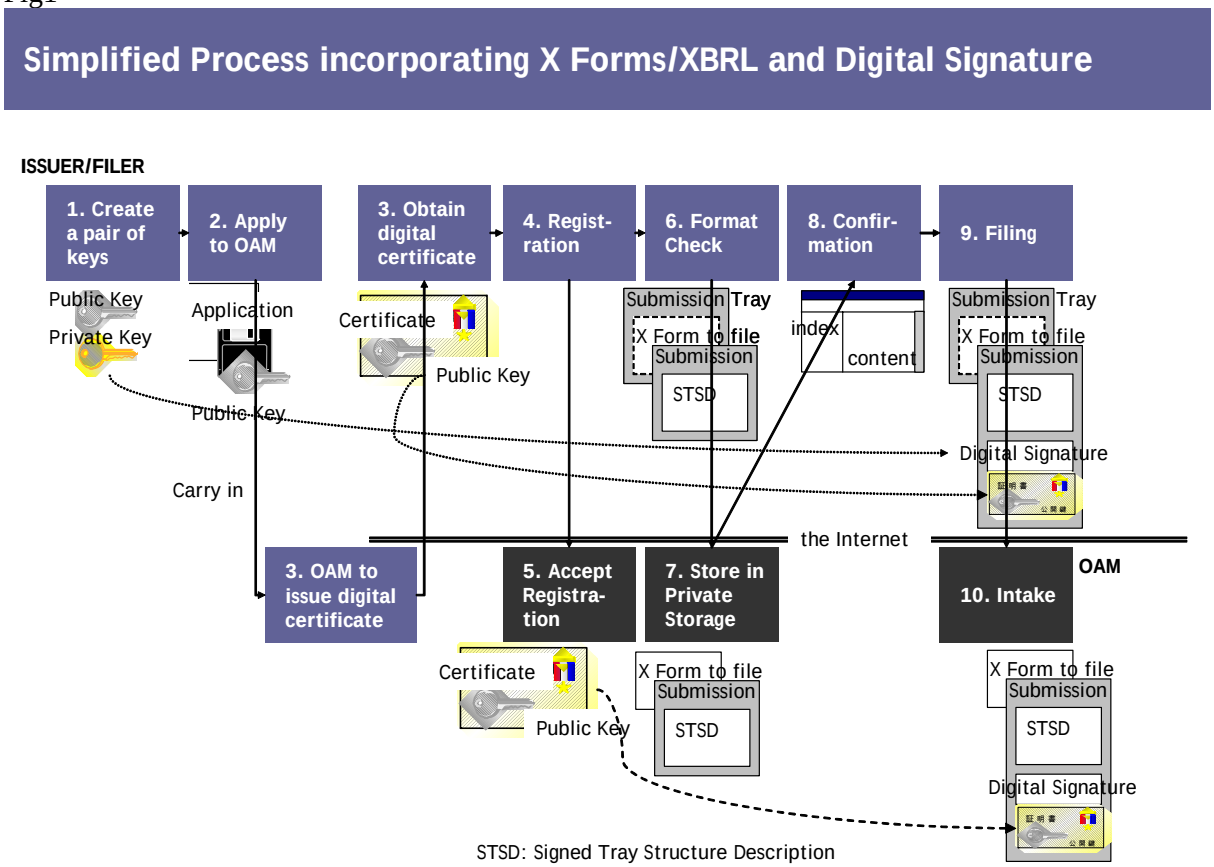
Consideration should be given to aligning the identification/authentication for TOD with the work of related registers such as those envisaged by the International Securities Association for Institutional Trade Communication. In this regard, IBM and NASD are active supporters of the Joint RDUG (Reference Data User Group) ISITC Europe sponsored project to create an International Business Entity Identifier Standard and registration process which maintains the hierarchies of relationships between IBEIs, and the further reference data which facilitates settlement and payment processes. Such IBEIs are recommended as the key to be used by all OAMs to provide an independent standard

identifier of information relating to issuers. They would play a further valuable role where OAMs provide added-value information beyond the strict scope of TOD.

It is important to state that the filer's access to this type of process should utilize commonly available or industry standard tools or facilities. The open X Forms-based technology mentioned above utilizes simple browser approaches, but the repository and filing process ought also to be able to accommodate filings using proprietary technologies which are so widespread as to be semi-standards: Adobe's Intelligent Document Platform being perhaps the prime example.

Current experience indicates that the security strategy outlined above is sufficient when deployed on the internet and that there is no need to deploy a private secure network. It is likely that using higher levels of authentication software will be more cost effective than use of secure networks. Although this always needs to be kept under review, we would recommend the ongoing use of the internet to avoid burdening issuers and particularly those who have to submit information on shareholdings with the costs of a private network.

Fig1



The technologies for ensuring security in transmission between OAMs through the integrated network would be essentially the same assuming that a messaging approach were to be adopted. This would apply equally whether a peer-to-peer arrangement or a hub-and-spoke architecture were to be used.

However, with a hub-and-spoke architecture an alternative approach is available which has the potential for significant cost savings. This alternative relies on data replication between the databases, driven by "watchers" monitoring state changes in the databases. It has strong in-built security through fully random encryption and other transmission security techniques, and also deploys transformation techniques that could simplify the management of heterogeneous architectures. There are proprietary elements to its technology, but an evaluation of its lower costs versus more open messaging approaches should be considered.

2.2. Repository Security.

Security of the data once in the repository is a dual problem: the OAM must have sufficient controls to prevent tampering with the data; but there is also the issue of long-term secure storage and disaster recovery capability

Access Controls and Permissions:

A secure repository such as an OAM needs to be managed to allow viewing access, but controlled to prevent malicious or unauthorised manipulation of the data. Commercially available products, which IBM and NASD have proven in service in OAM-like environments, effectively manage internal users as well as an increasing number of customers and partners through the Internet, addressing all four key areas of identity management:

- Identity lifecycle management (user self-care, enrollment and provisioning)
- Identity control (access and privacy control, single sign-on and auditing)
- Identity federation (sharing user authentication and attribute information between trusted Web services applications)
- Identity foundation (directory, directory integration and workflow)

Beyond this *barrier defence mechanism*, we would recommend that CESR also consider *active defences* which monitor attempts on the integrity of the data. These types of technologies are available commercially, which helps in controlling costs and in their interfacing with other elements of the infrastructure. Such enterprise risk management software facilitates the management of external and internal vulnerabilities. Operators can proactively address vulnerabilities and exposures in an enterprise context by harnessing intelligence across different security checkpoints to gain knowledge and insight into the root causes of these problems, and can use decision support to quickly upgrade security policies. Access to such outputs should be made available to the external monitoring committee that we propose in section 6 below. Such a capability:-

- Provides a single centralized view of security data across the enterprise
- Helps integrate security management from applications, operating systems and network devices
- Can reduce and classify security incidents to quickly identify and address real threats or vulnerabilities
- Helps provide business intelligence that enables organizations to proactively address their business risks using analytical historical reporting guides
- Enables the operator to realize the value of autonomic computing
- Povides predefined tasks to help quickly resolve denial-of-service attacks, viruses or unauthorized access
- Assists organizations with audit compliance (event data persistence)

An appropriate tool would monitor security incidents from a single web-based security console. The communications and control centre would centrally manage enterprise vulnerabilities and can help to centrally detect and assess attacks, threats and exposures by correlating security information and risk alerts from firewalls, routers, networks, host- and application-based intrusion detection systems, desktops, and vulnerability-scanning tool.

Data Retention and Disaster Recovery:

Beyond defence against malicious intrusion is the perhaps more important issue of operational resilience and strategic data retention.

For operational resilience we recommend CESR to set standards to ensure 24 X 7 availability and the ability to withstand a disaster to, for instance, the whole facility in which the OAM resides. High Availability/Disaster Recovery approaches are commercially available which, simply put, duplicate the database and communication systems, copy all data changes automatically, and "fail over" to the backup facility if the primary site goes out of action. Such capabilities used to rely on "disk mirroring" which restricted the distance of the back up site. Now such capabilities allow full geographic separation, with say the primary site in Poland and a backup in Italy.

Those operational resilience techniques can also be employed to ensure that failure of physical data storage devices on one site does not mean that the data is lost: it can be recovered from the back-up site or sites. Further layers of security against physical data loss include use of Write Once Read Many times (WORM) disks or tapes, with archive copies stored offsite. Protection against accidental data loss is further supported by a Records Management tool which ensures that the management of data retention is achieved by use of policy driven software which may be controlled by non-operational staff or potentially by the Competent Authority. A full range of such data retention capabilities is characteristic of current Enterprise Content Management software, and is available at modest cost. We recommend CESR set standards of data retention in the light of these capabilities.

2.3. Time Recording

Based on their knowledge of the use to which "structured" data can be put for regulatory surveillance or investment management purposes, IBM and NASD strongly recommend the use of input standards such as XBRL for major filings and templates encapsulated in e-forms for other types of regulated data. We see the use of XBRL as the natural corollary of the International Financial Reporting System; and we again refer to the work of ISITC and RDUG in sponsoring the use of e-forms in conjunction with the IBEI to facilitate to straight through processing of financial markets' supporting processes like settlements and payments.

Time stamping at each stage of the process of filing – reception and confirmation -, storage and publication we see as essential tools for managing the performance of the OAM operator, but more importantly for ensuring that information is available across Europe and to global investors on a level playing field.

We reiterate our belief that fast markets that approach real time are inherently safer from abuse, and the benefits of up to the minute market knowledge should be as widely available as possible within sensible cost limits. In this regard we think it particularly important that the standards set for the network should aim to make information available simultaneously. This in turn means that the integrated network must be able to transmit information to all OAMs or make it available from a central hub in close to real time so that the national availability of data is no better than the pan-European. Similarly OAMs receiving such international data must be able to make it available without delay.

Such expeditious handling of filings does however require that control checks are equally efficient. We would make the following recommendations:

- the principle of "right first time" should operate. Issuers, whether filing directly or through agents, must be clearly responsible for the quality of the substance and format of their filing
- support to filers for format accuracy should be provided by the OAMs making available an online test for the accuracy of the XML/XBRL which is the same as the test it will itself use on receipt of the filing: such tools are readily available
- checking the substance of the filing should however not be the responsibility of the OAM. They should accept the filing and make it expeditiously available, concurrently to its repository and to the integrated network. That general availability time stamp should be confirmed to the filer, and until that is received the information should be embargoed.
- There may however be a requirement by the competent authority to, for example assess whether to manage the market in the light of the information received. This should be handled either as a loop in the process sending the received filing to the competent authority and only moving to publication on return; or as a preceding process where all filings pass through the competent authority first – in which case the authority must have equivalent receipt and validation processes – and then passing to the OAM. In either case time stamping should be mandatory so that market discipline may operate on those checking processes.

- Notwithstanding the practicality of the checking process above which may be assisted by automated tools which are now becoming available for XBRL analysis of the substance of a filing, our own recommendation is that such checks should follow publication. Failure to file accurately should be an offence subject to regulatory sanction, and the analysis of filings should occur after publication.

2.4 Ease of Access by End Users

Recognizing, as does the Commission and CESR, that a well-informed market is an excellent 'regulator', creating a level playing field for all investors – institutional and retail, IBM and NASD consider that ease of access for end users, both investors and regulators, is a core value of any utility holding any form of capital market information. In the light of their knowledge of what are currently available technologies, they further consider that close to real time information systems are now cost effective, and provide the "fast markets" that are the best safeguard of transparency and equality of access.

However, with regard to the issue of minimum standards depending on the type of information to be accessed (e.g. where value added information is stored in the same repository as regulated information), we believe that the standards should not necessarily be the same, so long as there is clear identification of those types of information and the standards which apply to each category of information, and clear identification of the regulated information and that it does comply with EU standards.

In support of this statement we point to the fact that the Commission and CESR envisage that commercially operated OAMs may opt to carry not only regulated and unregulated raw information, but also value added information. The latter, almost by definition, will include a qualitative element that will render its supervision different in kind from that of raw data.

With regard to the language regime, there should be no problem in economically complying with a requirement that the access point should allow access in any European officially recognised language. Obviously the content can only appear in the language or language of submission, though the use of XBRL and XML should allow the universal ingestion and manipulation of any numerical data. Translation of the original submission should be seen as a value added activity by a value added information provider not as a core requirement of the OAM.

With regard to minimum standards in terms of the technical accessibility to the OAM, we concur with the view that availability should be 24 x 7, and that "easily accessible technologies" should be available to end users. We do however opine that an authority, probably the CSMC to which we make earlier reference, should, for purposes of certainty, regularly define. Similarly the standards applying to the support services should be established and regularly reviewed by the CSMC.

On the issue of the formats of information which must be supported, we first recognise that the human readable document is a basic minimum to be maintained for the foreseeable future. Ability to receive the document on paper rather than as a screen image is in our opinion already an added value service that should be provided at an extra cost, albeit that we believe that an efficient OEM could provide such a service at a modest one. Other capabilities such as having the XBRL "shredded" from the filing we also feel lie in the realm of added value services beyond the scope of these regulations, particularly as they would involve the OAM in an activity that carries risk (XBRL for instance only provides automatic interpretation of a subset of the total filing: there are optional approaches to certain elements, and the totality of the filing includes qualitative statements which require qualitative interpretation)

Notwithstanding the above qualifications in the use of XBRL, we consider that the core elements of extensive regulatory filings, and the more easily defined contents of the less extensive regulatory filings do provide a mechanism whereby information may be faithfully and expeditiously transferred from issuer to investor, added value provider, or regulator. There is, in our experience, a clear business imperative, and the cost to the issuer is not unreasonable. This cost to the issuer, however, is front end loaded. Experience shows that for all but the simplest enterprise mapping its own information accurately to the structure of the regulatory requirements is a significant project. Subsequent reporting once that initial work is completed and maintenance of the mapping is relatively minor. The benefits

of the initial work lie in significant reductions in attestation by directors and auditors, and most significantly in the reliability and ease of use of filings by the investment community. In these circumstances we consider that a regulatory imperative is necessary to "kick-start" the effective use of these input standards, which furthermore represent the logical outcome of IFRS.

On the matter of timeliness of access, we have above stated our strong commitment to enabling close to real time system. The Commission and CESR have implied that only practicality should stand in the way of accessibility without delay to all users. We recommend that that commitment to accessibility without delay be endorsed, with the responsibility for assessing its practicality devolved to the CSMC.

In its assessment of the funding mechanisms for the OAMS and their integrated network, CESR will be able to evaluate how far end user access could be made free of charge. IBM and NASD consider that sharing of infrastructure by member states will restrain the costs of the overall network of OAMs to the point where free access can be accommodated with acceptable charges on the public and on the issuers. If the actual deployment raises the costs to the point that user charging becomes necessary, we consider we have the technology to make micro-charging feasible.

3 Role of Competent Authorities

IBM and NASD in subsection 1.0 of this section 5.0 have already stated that the appropriate approach for the integrated network is for it to be subject to a Central Storage Mechanism Committee mandated by all the competent authorities and tasked with creating and monitoring the standards of operation of the pan-European network. The same approach should, we consider, be adopted for the supervision of any utility appointed by two or more member states. Such a CSMC could, in our view, be able to co-opt the necessary blend of regulatory and technical expertise to direct the operational management, whether in-house or outsourced, with appropriate regard to compliance and efficiency.

On the matter of the evolution of technical standards, we likewise consider a standing committee to be the appropriate mechanism for overseeing the overall standards of the set of OAMs and the integrated network.

These matters will be addressed in more detail in section 6.0 below.

4 Costs and Funding

As we have before stated, IBM and NASD consider that they have conjointly significant expertise in the area of regulatory filing systems which they are willing to use to assist CESR in its assessment of costs of setting up and operating OAMs. We reiterate that a significant proportion of those costs may be seen as fixed both in design, implementation and operation. We therefore would welcome the approach whereby two or more member states should share an OAM, particularly if this could be combined with a Central Storage Mechanism at the heart of a hub-and-spoke network.

5 Filing with Competent Authorities

The technical requirements of filing with Competent Authorities rather than OAMs are virtually identical, so may be considered covered by the relevant statements above. For further treatment of this issue see pages 24-25 below.

6.0 Role of Competent Authorities

The successful implementation of a system as envisioned by CESR will require the involvement of the Competent Authorities, to varying degrees, in a number of areas. Firstly, the appointment and recognition of OAM's will require an objective review of OAM applicants, as well as review and inspection of existing OAM's, to ensure that they comply with the minimum standards that are set for them (discussed above). Put differently, someone needs to have the responsibility to officially appoint Officially Appointed Mechanisms. This function is properly a function of the Competent Authorities, particularly in the absence of any self-regulatory organisation to fulfil this role.

Implied in this authority is the power to direct OAM's to modify their systems to bring them into compliance, and to suspend or revoke recognition as an OAM where necessary.

In addition to technical compliance, Competent Authorities should exercise oversight with respect to fair access and non-discriminatory pricing by OAM's. Access to information is of fundamental importance to the markets, and indeed the ability of the market to function effectively and fairly rests to a large degree on full and fair access to this information. While the *enforcement* of discriminatory practices may more properly lie with competition authorities, the *surveillance* of access lies best with the Competent Authorities who would hold the power to revoke or suspend official recognition.

As we note elsewhere, the adoption of joint OAM's by two or more Competent Authorities would help to improve the efficiency of the system and should be encouraged. Where this occurs, specific arrangements between the Competent Authorities will be necessary in order to ensure that sufficient oversight is conducted with respects to all aspects of the system. Such bilateral arrangements are best left to the Competent Authorities involved. This may in fact involve separate, bi-lateral Central Storage Mechanism Committees for the administration of the joint mechanisms, within the framework of a pan-European Committee as discussed elsewhere in this document.

This raises a larger 'stakeholder' issue. Even if there were no joint OAM's, and each Member State were to have its own OAM, other Member States would have an interest in the oversight of that OAM since information from the OAM will be accessed from across the EU. With mutual recognition of OAM's, reliance would be placed upon other Competent Authorities to exercise sufficient oversight and enforcement of the common standards. It is inevitable, however, that disputes would arise with respect to standards, access, and compliance, and we believe that these could be resolved in the first instance by the Central Storage Mechanism Committee described previously in this document.

With regard to the establishment of standards, it must be recognised that this is an on-going process. As markets evolve, regulatory requirements change, and technology progresses, new standards may be needed. At a minimum, existing standards will need to be reviewed periodically. This is a role properly reserved for the industry, in our view the Central Storage Mechanism Committee, although the official endorsement of standards by the Competent Authorities would be helpful in speeding the process. This endorsement should come from CESR or, more practically, from a subcommittee of CESR formed for this purpose.

Given the important role of the CSMC with respect to standards and to governance, we believe that it should operate under the mandate of CESR (see also our comments under 'Governance' on page 10). In this way, it will benefit on the one hand from valuable and timely expertise from industry and users, and on the other hand from the authority derived from its CESR mandate.

Appendix

Issue	Response
Issues on which CESR is invited to provide advice, with corresponding IBM/NASD views: drawn from section 3 of Mandate	
Preliminary issues In the light of the discussions held at the European Securities Committee (ESC) meeting of 26 May 2005, the Commission considers that the future European architecture for the storage of regulated information is likely to consist of a type of integrated network[5] of national databases allowing for sufficient flexibility and scalability, with the final objective of offering a one-stop-shop for end-users.	IBM and NASD concur that the final objective should be the creation of a one-stop-shop for users. While agreeing that the likely architecture will consist of a network of national databases, we note the openness of CESR and the Commission to flexible and scalable architectures whereby utilities may present a pan-European "front end view" to end users, while presenting a national "back end view" to issuers and national regulators.
Agreement on interoperability CESR should examine how an agreement on technical requirements to allow technical interoperability of Officially Appointed Mechanisms (OAMs) could be obtained and how to conduct ongoing control/supervision over such a joint project;	The EU competent authorities should create a dedicated Central Storage Mechanism Committee (CSMC) of national competent authorities, tasked with creating and monitoring the standards of operation of the Officially Appointed Mechanism(s). The CSMC should co-opt operators of the OAMs for technical guidance and issue standards. These standards would define the key input, security, timeliness and access criteria.
Cost and funding CESR should in particular make an analysis of the cost and funding implications for the Member States at the initial stages of the creation of such a EU-wide network.	We concur with CESR that "free access for retail users to regulated information is desirable". Building a low cost infrastructure therefore becomes a priority in order that a combination of public funding, charges on issuers (potentially through listing fees) and charges for commercial users (potentially as set out in the ELCID proposal for "push" feeds) may be set at acceptably low levels. However, should it be deemed necessary to charge retail users we would point out that technologies from the online media sales world would allow micro-charges to be made, and integrate easily into the Enterprise Content Management architecture we propose
Minimum quality standards of security to be complied with by the OAM. This issue should at least address the following points: (a) which should be the security standards should regulated information be sent to the storage mechanism only in electronic form and should regulated information be stored only in electronic form?	We strongly favour the mandating of electronic form both for submission and storage of regulated information. (a) Our view on the appropriate security architecture is covered in section 5 above and should be considered in conjunction with the closely related

Issue	Response
(b) whether special or additional security standards should be in place if an electronic network of national OAMs at EU level is created?	issue of filing of regulated information with Competent Authorities (Article19(1) of the Transparency Directive) – see below (b) The choices for security in a networked OAM environment are covered in Section 5 above
Minimum quality standards of certainty as to the information source to be complied with by the OAM, taking into consideration how the filing procedure with the OAM could take place. This issue should at least address the following points: (a) Whether it would appropriate to require issuers to file regulated information through electronic means only, types of electronic means that could be suitable taking into consideration the need to achieve certainty as to the source of information and the need to ensure integrity of content of regulated information (b) In this connection, how best to ensure authenticity of origin, in particular (but not only) if the information is to be filed with the OAM by an agent or representative of the issuer or other indirect methods;	Our model for filing procedures with an OAM are set out above and are based on extensive experience of similar utilities, notably SEDAR(Canada) and EDINET(Japan). Specifically: (a) A procedure supported by digital signatures, public/private keys and non-repudiation technologies and processes is a proven solution where electronic filing is the sole method of submission. Apart from the key issue of identifying the filer for control purposes, there is also the matter of making it transparent to end users, particularly regulators, what the broader identity of the issuer is and what if any relationship it bears to other legal entities. In this regard, IBM and NASD are active supporters of the ISITC sponsored project to create International Business Entity Identifiers and registers which maintain the hierarchies of relationships between IBEIs, and the further reference data which facilitates settlement and payment processes. Similarly NASD in particular is developing a database of approved brokers for issuers. We believe that an OAM should have linkage to or encompass the functionality of such databases to enrich the understanding of end users as to the context of the regulated information. (b) The use of IBEIs and similar data might also act as a system independent identifier to facilitate the security of identity in transmission from one OAM through the network to another.
Minimum quality standards of time recording to be complied with by the OAM, taking into consideration the organisation of the filing procedure with the OAM. This issue should at least address the following points: (a) Whether it would be desirable in order to	IBM and NASD view it as critical that regulated information should be available *simultaneously to all end users*, in order to achieve a true level playing field for investors. We therefore believe it to be most important that information should be released through the network at the same time as

Issue	Response
facilitate automatic processing of the regulated information, including the time recording procedure, to require issuers to use input standards (such as XBRL or similar formats) and templates (such as standard forms) for regulated information as a condition for the filing of information with the OAM; (b) The implications of any "content checking" procedure especially potential resulting delays.	it is released by an individual OAM. Time recording is necessary in order to prove this is the case. To support this approach, the filer should be prohibited from other publication of the regulated information until receiving positive notification from the OAM that the submission had been accepted and *retransmitted* to the wider network. Again, time recording of initial receipt and final retransmission would act as a market discipline on the OAM. On the issue of delay between submission at the OAM and release to end users, we believe that this should be minimized – again using time recording as a measure of an OAM's effectiveness – in order to reduce opportunities for market abuse. Within the context that the filer is responsible for the accuracy of the *substance of the filing*, the OAM's role is to ensure that *correct formats* have been adhered to. The OAM's procedure would reject submissions which failed format standards, but rejection of the filing for errors of substance would be a post-publication enforcement activity by the Competent Authority. Our preferred solution for this is to set standards to ensure that submissions are "right first time". Deployment of test tools which filers may use to pre-check their filings before final submission is a tried and tested mechanism for avoiding errors. The extension of such pre-emptive checking to include checks for correct XML/XBRL in electronic filings are already available, so should not inhibit use of input standards and templates. More complex use by Competent Authorities of automated tools for checking the substance of the filing should be treated as a post-publication discipline on the filer. There does remain the situation where the competent authority might need to take action as a result of the information imparted by a filing – to manage the market for example. In such cases, the competent authority should agree with the OAM a joint process whereby submissions are routed to the authority for approval and only after approval does the OAM publish the information and notify the filer.
Minimum quality standards of easy access by end users to be complied with by the OAM, taking into consideration the organization structure of OAM and the filing procedure. This	(a) Current records management and enterprise content management technologies, such as that at the heart of the ELCID architecture are designed to

Issue	Response
issue should at least address the following points: (a) whether there should be different minimum standards depending on the type of information to be accessed (e.g. regulated information under Directive 2003/6/EC and the Transparency Directive, and possibly additional information, such as the one to be disclosed under Directive 2003/71/EC, to the extent this non regulated information would be stored in the OAM) that may be obtained from an OAM;	allow a great deal of flexibility in the capture, storage, retention and access policies to apply to multiple categories of information. Use of input standards and templates will automate the categorization of submissions and thus greatly facilitate their subsequent management to different standards.
(b) minimum standards regarding the language regime of the access points for end users of interconnected OAMs at EU level in order to move towards a "one stop shop" for end users;	(b) Current access management processes such as the pub/sub and web access controls used in the ELCID architecture have proven capacity to support access for all European languages. The language used by the filer will remain unaltered, so full understanding by a user will still have that dependency. However, the use of input standards and templates will greatly facilitate the transparency of the core content of the filing, and could conceivably automate the interpretation of the simpler elements of filings especially where those were managed by templates.
(c) minimum standards in terms of technical accessibility to the OAM, including the type of technology used in the interface with end users (e.g. it should preferably be an easily accessible technology), the operational hours, the service support etc;	(c) Interoperability of end user access functionality with commonly available end user technologies is a core feature of the ELCID architecture. Its ability to support 24 x 7 environments is well proven. A further advantage of mandating solely electronic filings is that the store and access mechanisms may be easily replicated to provide High Availability and Disaster Recovery. The IBM/NASD contention is that a limited number of OAMs will find it easier to provide such assurance of availability even against serious risks by replicating their operating facilities across multiple geographies while still preserving low costs of operation. Service support could likewise be replicated.
(d) minimum standards in terms of the format of the information that can be accessed by end users, including in particular whether end users may be entitled to require receiving from the OAM a printed version of regulated information or may be entitled to obtain an electronic version only;	(d) While preferring to preserve complete electronic form in access as well as submission and storage of regulated information, it may be considered essential to preserve equality of access and social cohesion to make printed versions an entitlement. The technology to perform such a service is readily available, but will obviously carry a cost

Issue	Response
	and will be unable to achieve equality in timeliness.
(e) whether, in this regard, it would be appropriate to require issuers to use input standards (such as XBRL or similar formats) and templates (such as standard forms) for regulated information as a condition for the filing of information with the OAM to the extent that this would facilitate the searching of information, its subsequent manipulation by end users or by added value service providers.	(e) IBM/NASD strongly endorses the mandating of input standards and templates as a key element in facilitating end user search and manipulation of regulated information. Studies undertaken as part of engagements with other competent authorities and with major investment institutions show that automated ingestion and manipulation of market information is at the heart of modern investment approaches. It is most well developed with simple market price data. Methods of extracting the core numeric data from regulatory filings are eagerly awaited, and will greatly facilitate active investment in a broader spread of listed companies. We would again point to the importance of IBEIs in facilitating the combination of market intelligence from regulated information with other market data.
(f) minimum standards in terms of timely access to the regulated information, in particular whether the easy access principle requires that stored information, including price sensitive information, should be made accessible to end users without delay after reception by the OAM (see also paragraph 3(b));	(f) IBM and NASD strongly believe that fast markets where relevant information is available close to real time are the most transparent and subject to least market abuse. Protection of existing vested interests should not prevent OAMs from giving immediate access to all accepted filings to all end users (the issue of market management by competent authorities excepted). The ELCID architecture we propose is capable of providing such high speed access at reasonable cost which we are willing to discuss in detail with CESR.
(g) minimum standards in terms of cost of access to regulated information for end users;	(g) IBM and NASD concur with CESR that the cost of access for end users should be kept low, and there is a strong argument in making that a free service to retail users. Since costs must therefore be borne in the main by public support and charges on commercial users and on issuers, the cost of building and operating the OAM must be controlled. IBM and NASD believe that there is a major fixed cost in developing, implementing and operating such a utility which will tend to disadvantage member states with lower populations and market turnover. It therefore sees the advantage in member states sharing such infrastructures, so that

Issue	Response
	charges may be subject to standards based on equitable principles rather than a specific OAM's cost recovery needs.

Role of Competent Authorities in supervising OAMs' compliance with quality standards, for instance in the cases where two or more Member States would decide to officially appoint a joint mechanism for the central storage of regulated information. The technical advice could also give consideration as to whether competent authorities should have any role in adapting standards over time in case of technical developments and similarly.	In these circumstances, IBM and NASD recommend that the Competent Authorities of the relevant Member States would create a **Central Storage Mechanism Committee (CSMC**) of national competent authorities, whose functions would be to:
	• **Adopt and enforce standards** for implementation in Member States. The standards should include the format of the submission to the Central Storage Mechanism, the speed, controls etc.
	• **Licence a single multi-national contractor** to:
	  ○ **Operate the (single) Central Storage Mechanism** in accordance with parameters laid down by the national competent authorities.
	  ○ **Create a central website** through which basic information on all issuers is made available at no cost to investors.
	  ○ **Operate, potentially, on a cost plus basis** to make a return over and above the operating expenses and any re-investment requirements to enhance the operating model, subject to pricing oversight.
	However, As we note above in sections 5 and 6, IBM and NASD consider that management of the common standards to be applied by all OAMs, and the standards of the integrated network, all demand that a pan-European Central Storage Mechanism Committee be appointed.

Costs and funding DG Internal Market requests CESR to provide an assessment of the costs of setting up and operating OAMs that meet the standards listed in paragraphs 3.2.(1) to (4), and to deliver an interim report on this issue in April 2006.	IBM and NASD have already submitted to CESR and to the Commission outline costs for establishing a single Central Storage Mechanism. We remain ready to model with CESR's participation the likely costs for a variety of OAM structures: independent OAM utilities of various sizes; multinational OAMs sharing the development and/or implementation and/or operation of infrastructure and supporting activities; or the building of a pan-European information database to act as the hub of an OAM network supplying the international information component to national OAMs.
The filing of regulated information by electronic means with the competent authorities	Our comments above on filing with OAMs cover most of the issues in this section. We would add

Issue	Response
(Article 19(1) of the Transparency Directive) DG Internal Market requests CESR to provide technical advice on possible implementing measures on the filing of regulated information by electronic means with the competent authorities (Article19(1) of the Transparency Directive). The technical advice should concentrate on the following issues: (1) **Minimum quality standards** to be complied by the competent authorities, in particular in terms of security; of certainty as to the information source and of time recording. This issue should at least address the following points: (a) whether it would be appropriate to require filers (issuers, holders of voting rights etc) to use electronic means only for filing regulated information with the competent authorities, types of electronic means that could be suitable taking into consideration the need to achieve certainty as to the source of information and the need to ensure integrity of content of regulated information; (b) in this connection, how best to ensure authenticity of origin, in particular (but not only) if the information is to be filed with the competent authority by an agent (or similar) of the issuer or other indirect methods (c) whether it would be appropriate to require filers to use input standards and templates for drafting regulated information. (d) Implications of any validation procedure of regulated information on the recording of the filing.	however a number of additional comments 1)We set out that the role of the OAM is validating the filing should be confined to that of ensuring that the format supplied adhered to the required standards, and to then faithfully transmitting and storing that filing while positively notifying the filer of the stage of progress through the procedure. This would allow the OAM to focus on the efficiency and timeliness of the process of providing market transparency. The issue of the quality of the substance of the submission is however the responsibility of the Competent Authority. Before committing the submission as a final record further examination may prove appropriate. If this is the case then the initial submission should still be recorded to show what the market's knowledge was at the initial point. It may well be that timeliness is less important than thoroughness in those authorities processes; though the principle of simultaneity of disclosure to the market, in this case of regulatory action, must be adhered to. The technologies for ensuring authenticity of origin and integrity of content whether for OAM or Competent Authority are identical. Similarly the advantages to competent authorities in automating the surveillance processes require that filers of listed company information should be required to use input standards and templates with electronic submissions. Experience shows that electronic filing is in itself a net cost reduction for filers. In the case of templates such as X Forms the small added cost of complying with the constraints of the form are more than counter balanced by the benefits of certainty of compliance with the relevant regulation. The cost of preparing major regulatory filings to XBRL standards is being shown to be significant in the first year as corporate data structures are aligned with regulatory data dictionaries. The major work having been done in that first year, subsequent filings have proven easier and the additional benefits of certainty in attestation and compliance have been valuable.
Alignment of this procedure with the filing with the OAM. This issue should at least address the following points:	IBM and NASD believe that the most efficient approach is to completely align the initial filing

Issue	Response
(a) Possibility that the competent authorities act as interface for filing of regulated information with the OAM, whether the OAM is operated by the competent authority or not; (b) Interaction between the powers of the competent authorities to examine regulated information and take appropriate measures (cf. Article 24(4)(h)) and the availability of information to end users (see also section 3.2, paragraph 3(b).	process such that the OAM is acting as the receiver and repository of the initial submission on behalf of the Competent Authority. Subsequent regulatory actions could continue to use the OAM as the supporting database, given appropriate access controls and security. However, we believe that a replication of necessary information from the OAM to the Competent Authority's internal database is the more appropriate approach. It may be argued that use of an external agency such as an OAM would create the danger of loss of record of submissions in the event of catastrophic failure of the utility or legal entity. A sufficiently large organization would be able to afford at reasonable unit cost to build in disaster recovery processes, but this would place a burden on smaller member states. This argues for utility sharing between member states as we mention above. An alternative approach would be to build the network with a central hub that could act as the pan-European repository of record, or as a central disaster recovery mechanism.

