



Program Overview

Content Protection and Security Standard



04 Nov 2009

Revision 7.2



Background

Over a decade ago, the Content Delivery and Storage Association developed the world's first, independent and impartial audit certification system and related family of international standards, collectively called CDSA's Anti-Piracy and Compliance Programs (APCP).

With the support of the entertainment and media industry worldwide, CDSA has certified over 120 organizations on five continents in its cadre of APCP Standards. The APCP is the only industry-driven program recognized by major content holders and governments worldwide.

CDSA is your partner in protecting the security and integrity of intellectual property and related assets.

*Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org*



Objectives of CDSA's Anti-Piracy and Compliance Programs (APCP)

The Anti-Piracy and Compliance Programs and related Standards were developed to meet two key objectives:

- To support the health, growth and economic wellbeing of the entertainment and media industry by promoting sound security and anti-piracy compliance standards and practices.
- To help organizations across the supply chain adopt an open set of standards to protect the confidentiality, integrity and availability of intellectual property; our most valued asset.

By improving operational practices, organizations of any size or scope can minimize the risks associated with the handling, storage, and delivery of content, entertainment media, and other privileged assets. Unlike other programs, CDSA works in partnership with entertainment, media and content management organizations.

With four international offices (two in the United States, one in United Kingdom and one in Hong Kong), CDSA can meet the global needs of any organization regardless of locality.



APCP Family of Standards

To meet these objectives, CDSA offers three certification programs and related Standards (see Diagram 1):

- Copyright and Licensing Protection
- Packaging and Materials Standards
- **Content Protection and Security Standard – which includes Physical Security, Digital Asset Security and Post-Production Security.**

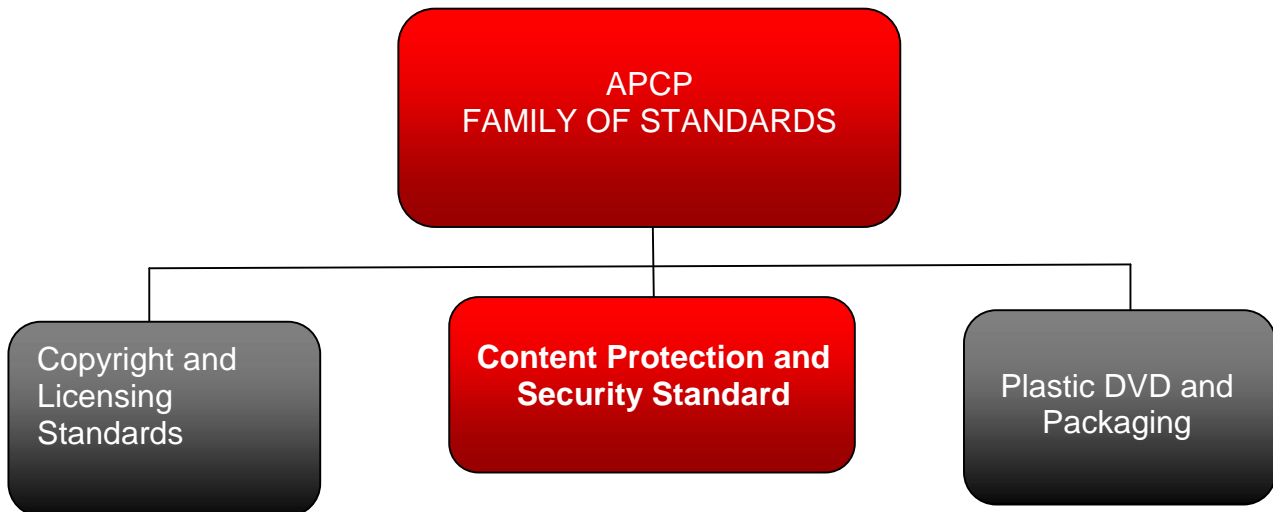


Diagram 1 – APCP Family of Standards

*Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org*



CDSA has pioneered a structured, yet practical accreditation processes to assist organizations to systematically manage its security and piracy risks. The program is called the Content Protection and Security Standard.

The framework focuses primarily on the security management of content, in all of its forms across the entire supply chain. It is comprised of:

- Risk-based assessments designed to identify and quantify risk.
- An internal and external Audit program.

The framework is designed to help organisations establish, implement, monitor, maintain and improve security management processes to better protect intellectual property and related assets.

Framework Model

The Content Protection and Security Standard is comprised of four levels:

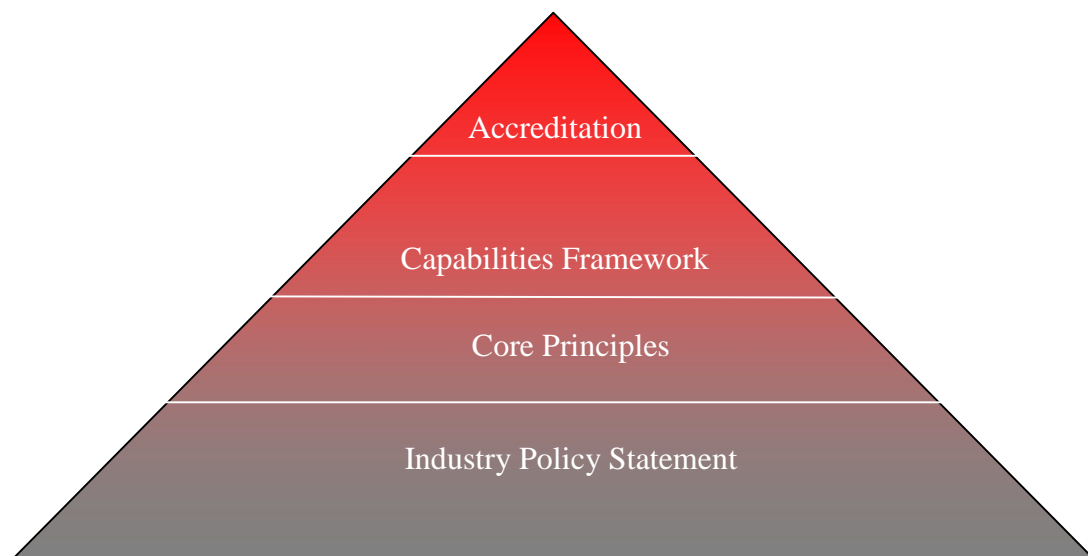


Diagram 2 – Model for the Content Protection and Security Standard Accreditation Program



Level 1 - Industry Policy Statement

“A global security and anti-piracy compliance program is essential to the protection of intellectual property assets. The security standard is industry-driven, effectively managed, and proportionately implemented to minimize risks associated with handling, storage and delivery of entertainment media and information content across the entire supply chain.”

Level 2- Core Principles

1. The security of Intellectual property is ultimately the responsibility of the intellectual property rights owner (IPR owner). To protect their most valuable asset, the IPR owner needs to manage risk within defined parameters.
2. IPR owners entrust their assets to internal and external resources for the purpose of creation, production, post production, manufacture and distribution. Whilst content is in their possession, there will be associated risks for which all have a common duty to mitigate such risks and ultimately protect the asset.
3. In order to function effectively and profitably, the entire media supply chain must be able to move content through the creative, manufacturing, storage and delivery process, confident in the knowledge that it is adequately protected from internal and external risks using a common set of agreed standards.
4. By adopting a set of open standards, the industry can secure its processes, display a strong resilience to those who may threaten it, and equip it to respond to any breach or lapse of security. It should enable proper treatment of possible risks, early identification and swift response to security incidents to minimise damage, and make necessary changes as needs arise.



Level 3 – Content Protection and Security Standard Capabilities Framework

The Content Protection and Security Standard Framework is comprised of the following seven (7) fields of competency, known as the 'Capabilities Framework' (CF):



▲ CF Requirements vary according to Security Risk Level



Level 4 – Requirements for Accreditation

CDSA’s knowledge and experience working within the supply chain has identified the need for a more granular yet practical approach to effective site security. To achieve this, CDSA has developed a series of “requirements” within each of the seven Fields of Capabilities.

The Schedule of Requirements forms the backbone of the accreditation process. The requirements must be reviewed and applied as necessary. This list may expand and adjust organically as the framework, available technologies and process requirements change, thus forming part of CDSA’s policy review, risk assessment, and ultimately accreditation.

Each Capability Framework (CF) Requirement can be found in the Guidance Document and is presented as follows:

- **Overview** of the Capability
- **Requirements**, based on the **CDSA Content Protection and Security Standard**, and
- **Evidence Necessary for Audit**.

The following are examples of CF Requirements, shown as follows:

| CF 5.4 INFRASTRUCTURE SECURITY MEASURES |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CF 5.4.1 ANTI-VIRUS |
| <p>Overview:</p> <p><i>Anti Virus technology now addresses a wide variety of threats; worms, Trojans, spyware, viruses and even the occasional root kit. Although the security industry classes this as Anti-Malware, users tend to refer to these groups with the original phrase ‘Anti Virus’, thus the name has been applied in this standard albeit that it encompasses these other threats. To comply with this implementation of this barrier, the organization must have an Anti Virus Strategy/Policy that defines:</i></p> <ol style="list-style-type: none"> 1. <i>Where Anti Virus software is to be deployed.</i> 2. <i>Where Anti Virus software is to not be installed/deployed.</i> 3. <i>Why it is not deployed everywhere (if applicable).</i> 4. <i>What countermeasures will be implemented where Anti Virus software is not installed?</i> 5. <i>The Anti Virus software must be updated at least weekly on clients and at least daily on servers.</i> 6. <i>Users must not be able to disable the Anti Virus software.</i> 7. <i>Anti Virus must perform on access scanning (on clients and servers).</i> 8. <i>Anti Virus must undertake background scanning at least once per month on clients and weekly on servers.</i> 9. <i>Anti Virus must be licensed and legally operated.</i> 10. <i>Anti Virus software must at least quarantine the malware (deletion is an option for the Anti Virus Strategy Policy).</i> |
| Required Actions |
| <p>Establish an Anti-Virus Policy or clause in an overarching Acceptable Use Policy.</p> <p>Establish a method which will convey the contents of the Policy to each user group.</p> <p>Establish a procedure to ensure that each user is fully aware of their responsibilities to comply with the Policy and solicit written consent to be contractually & legally bound by its conditions.</p> |
| Evidence for Audit |
| <p>Presentation of an Anti-Virus Policy or reference in an overarching Acceptable Use Policy.</p> <p>Presentation of the method, identification & verification that all employees & users of the corporate infrastructure have been made aware of the existence of a Secure Digital Asset Disposal Policy and written evidence that the employee has agreed to comply and be contractually & legally bound by its contents.</p> |

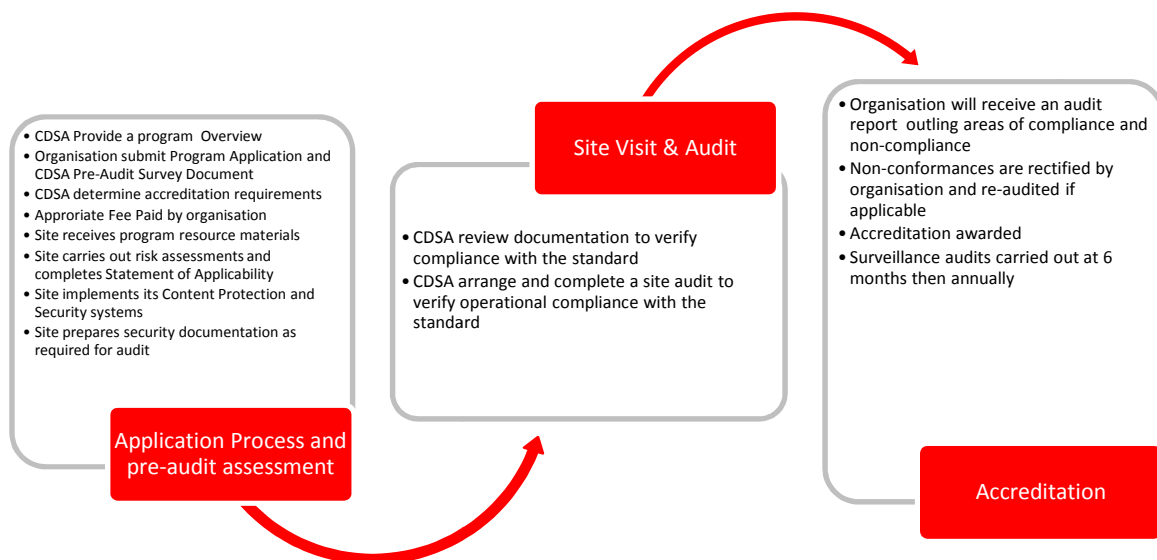
Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
 62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
 Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org



| |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CF 4 PHYSICAL SECURITY |
| CF 4.4 SECURING INTERNAL AREAS |
| <p>Overview:</p> <p><i>Site physical security measures may start with securing the asset and the environment it is contained within, and progresses to a defined secure perimeter. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to a variety of threats, including theft, fire, water, power failures, vibration, terrorism, vandalism, and environmental threats. Policies for preventing access to assets through segregation or procedure in combination with physical barriers and methods of securing assets (keypads, graded access cards etc.) complement other security measures.</i></p> |
| Required Actions |
| <p>CF 4.4.1 The organization must demonstrate its capability to secure and monitor the building(s), and internal areas containing content media or related assets, including vaults, safes, libraries, recording, mastering and mixing studios, control rooms, production areas, and data centers as applicable. Such secure areas must be identified.</p> <p>CF 4.4.2 Security controls must include:</p> <ul style="list-style-type: none"> ▪ Low visibility, secure areas, where possible ▪ Entry controls must be designed to allow only authorized personnel into secured areas. <p>CF 4.4.3 Access control measures that address:</p> <ul style="list-style-type: none"> ▪ Staff access control ▪ Visitor registration and access control ▪ Contractor and maintenance personnel registration and access control ▪ Other third party access control ▪ Monitoring of secure areas access ▪ Closed door policy to prevent unauthorized access <p>CF 4.4.4 The organization must be capable of effectively monitoring, preventing, detecting and mitigating risks relating to a variety of threats, including theft, fire, water, power failures, vibration, vandalism, environmental threats, and other natural or manmade disasters.</p> <p>CF 4.4.5 The use of equipment and other devices [e.g., fire/smoke detectors, vibration detectors, humidity detectors, uninterruptible power supply (UPS), etc.] to monitor and control the secure environment.</p> |
| Evidence for Audit |
| <p>Visual inspection of security methods employed to secure and monitor the building(s) and internal areas</p> <p>Inspection of visitor logs</p> <p>Inspection of monitoring, mitigation equipment in relation to environmental threats.</p> <p>Visual inspection of fire/smoke alarms, humidity detectors and other monitoring equipment.</p> |

Content Protection and Security Standard Accreditation Process

This brief outline should help you understand the steps necessary to achieve site accreditation. CDSA will be available throughout the process to provide guidance.



Step 1 Application

CDSA will provide a schedule of requirements together with the necessary application forms and pre-audit survey document.

Organisations seeking accreditation must submit an application (application form and a pre-survey questionnaire document).

CDSA will ascertain the potential and actual security risk level posed by the organisation through a review of the documentation completed by the applicant:

- **Program Application** provides general site and business information.



- **Pre-Audit Assessment Survey (relevant sections only to be completed)** helps to identify primary risks posed by operational activities and workflow, security control requirements and objectives, technical and business and the nature of the content and related assets in its custody.

Using this data, CDSA will determine the appropriate audit program for the organisations according to its size and activity.

The organisation will then commit to the program and pay the appropriate fee to CDSA.

A pack of resource materials will be provided to the applicant company, to include:

- Statement of Applicability
- Physical or Digital Guidance Documentation (dependant on the organisations services)

Audit Programs

There are two audit programs, based upon the potential and actual risks posed by the organisations activity and the complexity of its operations. The level determines the Capability Framework requirements that must be implemented by the organisation, the extent and formality of required documentation (e.g. security policies, standards, specifications, procedures and records) that must be in place to achieve accreditation through CDSA's certification audit process.

- **Standard Security Risk Level** – Where the security risk exposure and impact are low. Accordingly, the site must demonstrate applied methodologies in all Capability Framework (CF) areas, but may not be required to have formal documentation addressing all CF areas to become CDSA accredited.

Activities that require this level of certification may include but not exclusively: distribution, freight forwarding and storage of completed or post release product; printing and the merchandising of non-sensitive component parts or peripheral materials.

At the Standard Security Risk Level, the CDSA certification on site audit can typically be completed in approximately one (1) day.

*Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org*

- **Enhanced Level** – Where the security risk exposure and impact is high the site must demonstrate formal and proficient methodologies and documentation in all Capability Framework (CF) areas to become CDSA accredited.

Activities that require this level of certification may include, but not exclusively: content creation, origination, editing, authoring and subtitling/dubbing, the manufacture and replication of pre- and post release content, pre-release promotional activities and/or the handling, storage, transmission and distribution of digital content.

Due to the scope, depth and extent of the content security program at the Enhanced Security Risk Level, the CDSA accreditation on site audit can be completed within 1.5 – 3 days.

Pre Audit Activity

Using the guidance documentation provided, the organisation will complete a risk assessment and a **Statement of Applicability** which summarises all mandatory security requirements that must be met. This documentation will stipulate the types of controls in place or where appropriate give an explanation and justification for any exclusion(s).

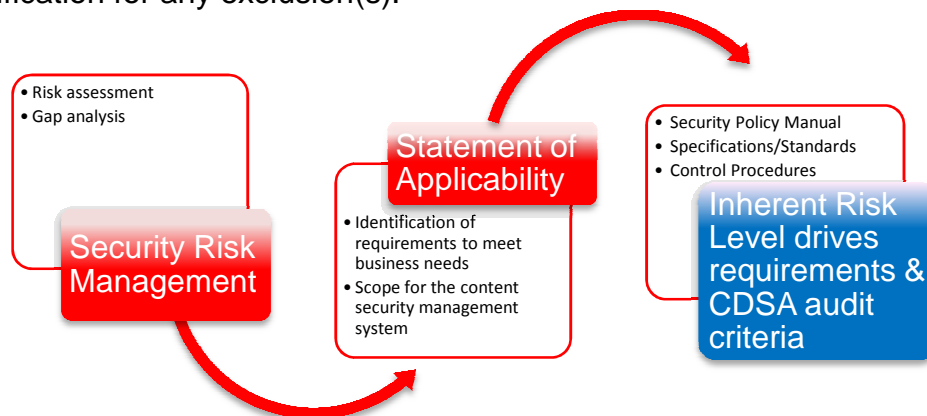


Diagram 3 – Determining the appropriate Security Risk Level

Example Statement of Applicability (SoA)

*Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org*

Upon completion of the requisite site documents, by the applicant, a site audit will be arranged and conducted by CDSA.

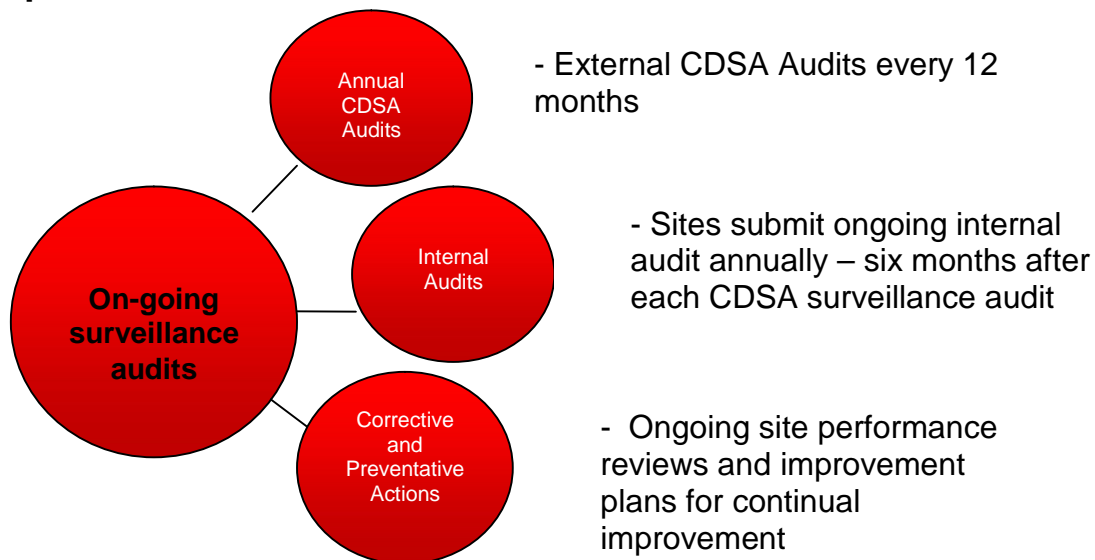
Step 3 Audit Report & Further Review

The applicant will receive an Audit Report which will contain details of all compliances and non compliances together with other conclusions and recommendations.

If one or more major or systemic non-compliances are identified during the initial accreditation audit, then a re-audit may be required. A re-audit fee must be paid prior to a follow-up visit for this purpose. When minor non-compliances are identified, the applicant must submit corrective action plans to address them within 30 days of the audit. These plans will be reviewed and approved by CDSA auditors for suitability.

If the initial audit is successful site accreditation is achieved, this accreditation status will be valid for 6 months¹ following which a further audit is required to confirm compliance with procedures.

Step 4 Annual Surveillance Audits



¹ Sites already participating in the antipiracy program will achieve accreditation for 12 months.



After the initial accreditation audit, the site will maintain its status through an annual CDSA audit called the Surveillance Audit.

Organisations must submit internal audits, to CDSA, 6 months following each surveillance audit.

Next Steps

To discuss specific requirements and application into the Content Protection and Security Standard contact your regional ACP Director for more details:

North, Central and South America

Linda Dyson

3455 N Desert Drive, Suite 3209
East Point, GA 30344 USA
Tel: +1 (404) 349 9600 Fax: +1 (404) 349 4499
E-mail: ldyson@contentdeliveryandstorage.org

Europe, Middle East and Africa

Peter Wallace

One Heddon Street
Mayfair
London
W1 4BD
Tel: +44 (0) 7850 331033
E-mail: pwallace@contentdeliveryandstorage.org

Asia

James Wise

22/F, 3 Lockhart Road, Wanchai, Hong Kong, SAR
Tel: +852-2863-6980 Fax: +852-2290-9111
E-mail: jwise@contentdeliveryandstorage.org

*Copy right ©2009 Content Delivery and Storage Association
(Formerly the International Recording Media Association - IRMA)
62 Snyderstown Road, Suite 301 • Hopewell, New Jersey 08525 USA
Tel: +1-609-279-1700 • Fax: +1-609-279-1999
www.contentdeliveryandstorage.org*