TRUSTED PARTNER NETWORK

POWERED BY MOTION PICTURE ASSOCIATION

MPA Content Security Best Practices Version 5.0: Objectives and Methodology

Author: Crystal Pham

Contents

INTRODUCTION

The purpose of this document is to outline the objectives and methodology used to develop the MPA Content Security Best Practices Version 5.0 to meet the industry's evolving security needs, address industry-specific challenges and provide clear information for all stakeholders involved in Content Security.

The Media and Entertainment industry, including Production and Marketing, has challenges that some other industries don't typically face. Decision-making often requires information quickly to make critical decisions. Volumes are often large and need to be managed accordingly. Service Providers vary in size and scope, from individual contributors to multi-million-dollar companies. Technological advancements require rapid evaluation and adoption. Throughout it all, security continues to be of utmost importance. TPN understands the distinct challenges and the importance of enabling the Content Owners freedom throughout the creative process, while also balancing the need for Content Security.

DELIVERABLES AND OUTCOME

The MPA Content Security Best Practices v5.0 are published with 64 Best Practices and Implementation Guidance, including the following updates and additions:

- Best Practices, including Application and Cloud
- Implementation Guidance, including Application and Cloud
- Definitions for Best Practices and Implementation Guidance
- Security Domains
- Security Topics
- Site vs Cloud Identifier
- Control Framework Mapping
- Glossary

DECISION-MAKING PROCESS

TPN received feedback from a sizable cross-section of Content Owners, Service Providers, and Assessment Companies. We reviewed every single comment and question and understandably, perspectives were wide-ranging, and opinions were strong. For example, some felt the same Best Practice should be a requirement, while others felt the Best Practice could never be met, due to particular business reasons. Similarly, some felt a Best Practice or Implementation Guidance were not prescriptive enough, while others felt they were too prescriptive.

Ultimately, TPN weighed all feedback to meet the greatest need across the wide variety of Service Provider types, as well as meet the security needs of the industry.

BACKGROUND

For more than three decades, the MPA has managed Content Security assessments on behalf of its member companies: Netflix Studios, LLC; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Walt Disney Studios Motion Pictures; and Warner Bros. Discovery Inc. Assessments were performed using a standardized set of MPA Site Best Practices and Common Guidelines. In 2018, the MPA and Content Delivery and Security Association (CDSA) created the TPN and in 2021, TPN became wholly owned by MPA.

TPN is a global, industry-wide program created to unite the Media and Entertainment community, comprised of Content Owners, Service Providers, and Assessors, to avoid leaks, breaches and hacks of its most prized asset, its content. Content assets can include media such as video, audio, storyboards, or photos as well as other types of assets such as scripts, subtitles, budgets, and contracts. TPN and its members, define the MPA Content Security Best Practices for use by the industry, and to increase security awareness, preparedness, and capabilities to secure content throughout the content lifecycle. The MPA Best Practices establish a single benchmark of minimum-security preparedness for all Service Providers. In turn, TPN runs an assessment program against the Best Practices to determine a Service Provider's security status. By creating a single, global directory of "trusted partner" Service Providers and their security status, Content Owners can make independent, risk-based business decisions more easily.

Now that the Media and Entertainment industry has transitioned to cloud-based applications, supply chains and workflows and the MPA Content Security Best Practices have been updated in response to the rapid growth in multi-layered hybrid and cloud-native supply chains and workflows.

STAKEHOLDER COMMUNITY

Content Owners are organizations that produce, manage, license, and/or distributes content. The Content Owner is ultimately responsible for maintaining the content's security during its lifecycle including prior to its intended initial release. Content Owners have unique risk profiles, that can be enterprise-wide, or by specific business line, process/workflow, project/title, or asset type.

Service Providers are a critical part of the content creation and distribution supply chain ecosystem that require standardized Content Security Best Practices and an efficient security assessment process that is consistent across the industry.

Assessors are TPN-accredited individuals who perform site and cloud assessments of a Service Providers' security preparedness measured against MPA Best Practices and capture findings. They are responsible for gathering information, validating evidence, and providing an assessment of a Service Provider's security status.

OBJECTIVES

Quality is Key

- Maintain highest quality standards to provide a single benchmark of minimum-security preparedness.

Plan for Variability

- Create a framework that accommodates multiple stakeholder perspectives and varied processes, technologies, infrastructures, workflows, and content types.

Simplify When Possible

- Provide clear, concise, practical, and comprehensive Best Practices that are easy to understand and implement.

Flexibility Matters

- Create a structure that can consider and continue to grow with industry evolution.

METHODOLOGY

The MPA Site Best Practices and Common Guidelines v4.10 include 263 Best Practices. They were developed for site-based Service Provider assessments, and specifically targeted post-production facilities and workflows. Over time, some cloud and work-from-home Best Practices were added. The TPN team also received 111 proposed Application and Cloud controls from a third-party assessment company, Convergent Risks.

The following details the strategy and approach deployed during the creation of v5.0 with reference to the above outlined objectives.

1. Consider Multiple Perspectives

We partnered with the Cloud Security Alliance (CSA) to receive feedback from their internal subject matter experts. Using Convergent Risks' proposed App/Cloud controls, we launched a pilot Cloud assessment program to seek feedback from a representative sample of Service Providers in the industry. Each Service Provider was invited to provide feedback to TPN on the App/Cloud controls for TPN's consideration.

Upon completion of the v5.0 first draft, we solicited feedback from over 20 industry organizations, including industry assessment Companies Convergent Risks, International Security Evaluators (ISE), [re]Design and Richey May.

All MPA members as well as other Content Owners provided detailed feedback to TPN also.

2. Ensure Relevancy

With the addition of Application and Cloud Security, TPN took the opportunity to review every Best Practice to determine if it was still relevant to current workflows, security requirements, and today's technology and infrastructure. We asked ourselves "Does the Best Practice help address today's threat landscape? If so, should it be expanded, be more specific to help clarify, or be re-written to specify the security requirement?" If it did not meet these requirements, the Best Practice was either removed or consolidated with other related and relevant Best Practices.

3. Focus on Security

TPN's intent with developing the Best Practices was to help Service Providers secure content. We mapped the MPA Content Security Best Practices v5.0 against industry recognized security frameworks, including AICPA TSC 2017, CSA CCM v4.0.3, ISO 27002-2022, and NIST 800-53 Rev. 5. This provided more structure and strengthened standardization.

Through our process, we also identified several Best Practices in v4.10 that were a part of managing the business (e.g., segregating replication lines) and did not focus on security. As a result, we removed these Best Practices, while updating others to better focus on our objectives.

4. Provide Clarity

During this process, we received feedback from TPN community members, and the most common was, "What is the difference between a Best Practice and an Implementation Guidance?". To help answer this question, TPN developed the following definitions:

- **Best Practice**: Minimum requirements where all components need to be fully met to fulfill the overall Best Practice.
- **Implementation Guidance**: Supplemental recommendations for Best Practices implementation. These are not requirements.

5. Reduce Redundancy

TPN recognized that the MPA Site Best Practices and Common Guidelines v4.10 included the same questions in multiple areas. Not only did these repetitive questions create fatigue during the assessment process, but they did not provide additional value. Whenever and wherever possible, TPN grouped related Best Practices and Implementation Guidance to remove duplicative questions.

6. Recognize Differences

To accommodate different service types, organization size, locations, and business requirements, the cadence of reviews and updates were changed from specific timelines (e.g., quarterly, or annually), to "regularly as appropriate". It is now the responsibility of the Assessor to capture the scope and cadence with the Service Provider, and for the Content Owner to determine the cadence needed to meet the security needs of their risk profile.

7. Site vs Cloud

Many workflows today are a hybrid of both Site and Cloud. It was critically important to integrate the new Cloud Security Best Practices with the existing MPA Site Best Practices and Common Guidelines. The updated MPA Content Security Best Practices v5.0 now specify either "Site only", "Cloud only", or both "Hybrid (both Site and Cloud". The "Hybrid" classification allows for a question to be asked once, answered once, and applied to both Site and Cloud.

8. Domains and Topics

TPN reviewed v4.10 Security Domains, Security Areas, and Security Topics. For v5.0, we updated the Security Domains to better reflect the intended objectives of the Best Practices and Implementation Guidance and to support the addition of Application and Cloud Security. See table below, sorted in alphabetical order.

Security Domains v4.10	Security Domains v5.0
Digital Security	Operational Security
Management Systems	Organization Security
Physical Security	Physical Security
	Technical Security

During review, TPN deemed the Security Area layer as unnecessary, and it was removed.

Security Areas v4.10
Asset Management
Content Management
Content Transfer
Facility
Infrastructure
Organization and Management
Transport

The v4.10 Security Topics numbered 47 in total and were overly complicated. We streamlined the v5.0 Security Topics to 12 which greatly simplifies the assessment process.

Security Topics v4.10	Security Topics v5.0
Account Management	Access Control
Alarms	Asset Management
Authentication	Cryptography
Authorization	Incident Management
Background Checks	Information Systems
Blank Media/Raw Stock Tracking	Logistics
Business Continuity & Disaster Recovery	Monitoring
Cameras	Network Security
Change Control & Configuration Management	Personnel Security
Client Assets	Policies & Procedures
Client Portal	Risk Management
Confidentiality Agreement	Vulnerability Management
Content Tracking	
Disposals	

Electronic Access Control
Entry/Exit Points
Executive Security Awareness/Oversight
Firewall/WAN/Perimeter Security
I/O Device Security
Identification
Incident Response
Internet
Inventory Counts
Inventory Tracking
Keys
Labeling
LAN/Internal Network
Logging and Monitoring
Mobile Security
Packaging
Perimeter Security
Policies and Procedures
Receiving
Risk Management
Searches
Security Organization
Security Techniques
Segregation of Duties
Shipping
System Security
Third Party Use & Screenings
Transfer Device Methodology
Transfer Systems
Transport Vehicles
Visitor Entry/Exit
Wireless
Workflow

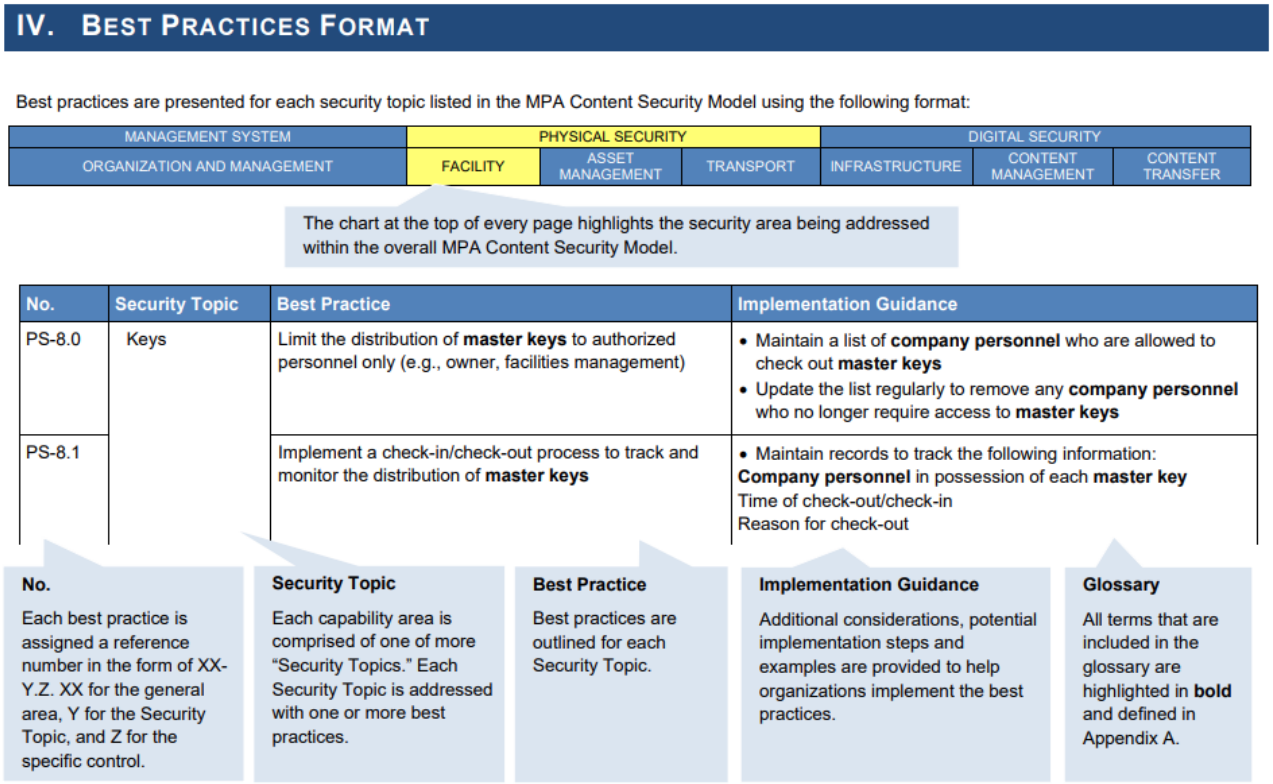
9. Glossary

As the scope of the MPA Content Security Best Practices v5.0 expanded to include Application and Cloud and the evolution of industry terms and technology continues, the Glossary was updated accordingly. The Glossary now contains key terms commonly used in the Media and Entertainment and Information Security industries related to Operational, Organizational, Physical, and Technical Security.

10. Functional Format

The MPA Site Best Practices and Common Guidelines v4.10 were published in a PDF format. The 105 pages were difficult to sort, filter, and incorporate into Service Provider's Standard Operating Procedures (SOPs). The updated MPA Best Practices v5.0 is published in an Excel format. When downloaded, this enables the user to sort, filter, and incorporate into the Service Provider's SOPs if needed.

MPA Site Best Practices and Common Guidelines v4.10



IV. Best Practices Format

Best practices are presented for each security topic listed in the MPA Content Security Model using the following format:

MANAGEMENT SYSTEM	PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

The chart at the top of every page highlights the security area being addressed within the overall MPA Content Security Model.

No.	Security Topic	Best Practice	Implementation Guidance
PS-8.0	Keys	Limit the distribution of **master keys** to authorized personnel only (e.g., owner, facilities management)	• Maintain a list of **company personnel** who are allowed to check out **master keys** • Update the list regularly to remove any **company personnel** who no longer require access to **master keys**
PS-8.1		Implement a check-in/check-out process to track and monitor the distribution of **master keys**	• Maintain records to track the following information: **Company personnel** in possession of each **master key** Time of check-out/check-in Reason for check-out

No.

Each best practice is assigned a reference number in the form of XX-Y.Z. XX for the general area, Y for the Security Topic, and Z for the specific control.

Security Topic

Each capability area is comprised of one of more "Security Topics." Each Security Topic is addressed with one or more best practices.

Best Practice

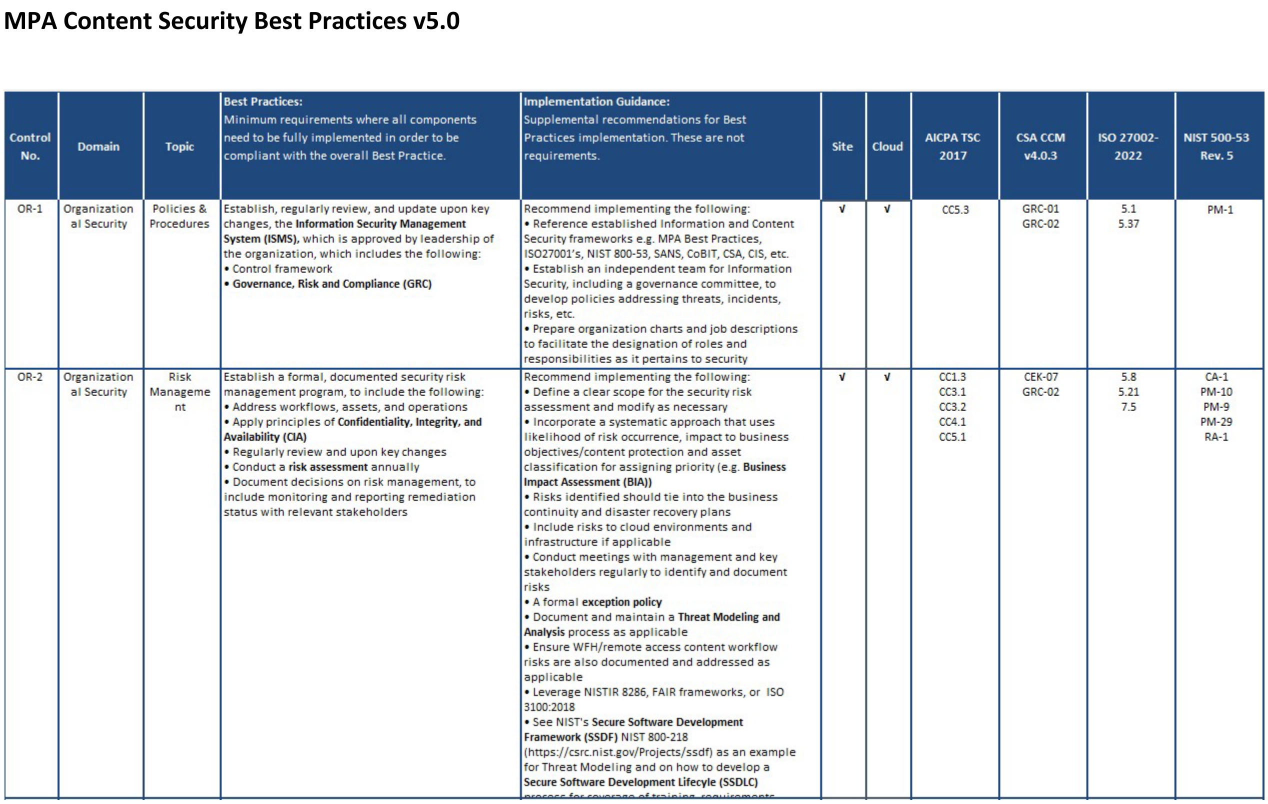
Best practices are outlined for each Security Topic.

Implementation Guidance

Additional considerations, potential implementation steps and examples are provided to help organizations implement the best practices.

Glossary

All terms that are included in the glossary are highlighted in **bold** and defined in Appendix A.



MPA Content Security Best Practices v5.0

Control No.	Domain	Topic	**Best Practices:** Minimum requirements where all components need to be fully implemented in order to be compliant with the overall Best Practice.	**Implementation Guidance:** Supplemental recommendations for Best Practices implementation. These are not requirements.	Site	Cloud	AICPA TSC 2017	CSA CCM v4.0.3	ISO 27002-2022	NIST 500-53 Rev. 5
OR-1	Organizational Security	Policies & Procedures	Establish, regularly review, and update upon key changes, the **Information Security Management System (ISMS),** which is approved by leadership of the organization, which includes the following: • Control framework • **Governance, Risk and Compliance (GRC)**	Recommend implementing the following: • Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO27001's, NIST 800-53, SANS, CoBIT, CSA, CIS, etc. • Establish an independent team for Information Security, including a governance committee, to develop policies addressing threats, incidents, risks, etc. • Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to security	√	√	CC5.3	GRC-01 GRC-02	5.1 5.37	PM-1
OR-2	Organizational Security	Risk Management	Establish a formal, documented security risk management program, to include the following: • Address workflows, assets, and operations • Apply principles of **Confidentiality, Integrity, and Availability (CIA)** • Regularly review and upon key changes • Conduct a **risk assessment** annually • Document decisions on risk management, to include monitoring and reporting remediation status with relevant stakeholders	Recommend implementing the following: • Define a clear scope for the security risk assessment and modify as necessary • Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection and asset classification for assigning priority (e.g. **Business Impact Assessment (BIA))** • Risks identified should tie into the business continuity and disaster recovery plans • Include risks to cloud environments and infrastructure if applicable • Conduct meetings with management and key stakeholders regularly to identify and document risks • A formal **exception policy** • Document and maintain a **Threat Modeling and Analysis** process as applicable • Ensure WFH/remote access content workflow risks are also documented and addressed as applicable • Leverage NISTIR 8286, FAIR frameworks, or ISO 3100:2018 • See NIST's **Secure Software Development Framework (SSDF)** NIST 800-218 (https://csrc.nist.gov/Projects/ssdf) as an example for Threat Modeling and on how to develop a **Secure Software Development Lifecyle (SSDLC)** process for coverage of training, requirements	√	√	CC1.3 CC3.1 CC3.2 CC4.1 CC5.1	CEK-07 GRC-02	5.8 5.21 7.5	CA-1 PM-10 PM-9 PM-29 RA-1

CONTINUOUS FEEDBACK PROCESS

TPN captured all stakeholder feedback and will continue to review and consider these comments for future updates. Additionally, we will monitor, review, and analyze progress made by the industry on the MPA Content Security Best Practices v5.0.

We look forward to working with the community on an ongoing basis for future enhancements. In the spirit of our collective forward momentum, collaboration, and innovation, the MPA Content Security Best Practices are now based on a solid foundation that will provide the industry with its most comprehensive roadmap for continuously addressing Content Security.