TUV RHEINLAND - HOMAI HOLOGRAM SAFETY AND SECURITY MANAGEMENT SYSTEM

“A road map to upgrade hologram suppliers’ facilities / process”

International Standards 2011

Foreward

Pradip Shroff
President, HoMAI

Dear Esteemed Members,

I am pleased to present you the "TUV-HOMAI Hologram Safety & Security Management Systems (HSSMS)". This project was initiated as per the approval given at the AGM in June 2010, with an aim to provide a document for developing a road map to upgrade hologram suppliers' facilities / process.

The TUV team visited some of the HOMAI members' facilities to get first hand understanding of Hologram manufacturing and security systems being currently used. TUV team has done extensive research on global standards and practices in preparation of the preliminary document. The final document was finalised by the Governing body after due deliberations and was presented and approved at the AGM in July 2011.

All HOMAI members can now approach TUV Rhineland team (details given in the report) and work with them to achieve certification and get recognised. Our partnership with TUV is a critical element in this certification process as TUV is an independent body well recognised all over the world. We are all suppliers of solutions against counterfeiting and hence our customers would be happy with this independent impartial assessment of assurance that we can give to our customers. We should all use this certification as a way to differentiate ourselves.

I now look forward to all members implementing this certification.

With Best Regards,
Pradip Shroff
President, HoMAI

Foreward

C.Ebenezer Bobson
Country Head – Business Risk Management
TUV Rheinland India

It gives me immense pleasure in being part of this Process Management initiative for Hologram Manufacturing Industries focusing on Safety & Security. The **TUV Rheinland – HoMAI** – Hologram Safety & Security Management System standard is an holistic standard which includes Quality Management System, Information Security Management System, Supply Chain Management, Brand Protection Management System, Data Protection requirements, Prototype Protection Management system, Business Continuity Management System and also incorporating best practices for the domain of Hologram manufacturing globally.

This standard will be a comprehensive and consolidated approach towards implementation of an effective Safety & Security management system.

The organization implementing this Holistic Standard will be benefitted by

- Best Practices Implementation to achieve global work environment
- Effective Risk assessment & Business continuity management practice implementation
- Effective Incident management & Risk treatment

The standard covers solely the risk management of confidentiality, integrity and availability considering safety & security across the process of manufacturing”.

The certification to this standard emphasis the organization demonstrated ability to consistently meet the applicable statutory, regulatory, and customer requirements of Hologram Manufacturing process focusing on Safety & Security at its highest level of Effective Implementation.

I hereby encourage all the members of HoMAI to participate in the initiative wholeheartedly to implement the standard in your esteemed organization and reap the benefits & to leverage the brand value to be a part of global supply chain.

C. Ebenezer Bobson
Country Head – Business Risk Management
TUV Rheinland India

Acknowledgements

A number of the processes and tools used in this document are taken from various sources provided by HOMAI member companies such as Alpha Lasertek, Holostik India, Holoflex, PRS Permacel & Uflex.

Many individuals contributed to this document in one way of another and we would like to thanks

G S Dhillon, from AlphaLasertek

U K Gupta, Ritesh Rupramka, Nanveet Goyal & Sunit Gupta from Holostik India

Dr. S N Bhattacharya and Dr.Anant Agashe from PRS Permacel

Manoj Kochar, Shouvik Dutta and Nasir Kamal from Holoflex

Arun Agarwal from Kantas Track Pack

R D Surana from Everest Holovision

G P Pathak from Uflex Ltd

Enrico Ruhle, E Bobson, S.Mohan Kumar, C.R.Parthasarathy from TUV Rheinland India

C S Jeena for Co-ordination and editorial solutions

Our special thanks to Luv D Shriram for being headed the drafting committee and to Pradip Shroff for initiated the project, as without them the project could not be accomplished.

Finally to all HoMAI members for their continued trust, encouragement and support.

INTERNATIONAL STANDARD

HSSMS

TUVR-HoMAI

HOLOGRAM SAFETY AND SECURITY MANAGEMENT STANDARD

STANDARD VER 6.2, AUGUST 2011

Version No.6.2 16th August 2011

TÜVRheinland®
Precisely Right.

Confidential © Copyright 2011 TUVR_HOMAI Hologram Safety and Security Management Standard

Contents

HSMS

0. Introduction

General

The **TUVR-HoMAI HOLOGRAM SAFETY AND SECURITY MANAGEMENT STANDARD** is developed by **TUV Rheinland (India) Pvt. Ltd.,** an organization engaged in third party certification and testing in various domains and catering to the needs of manufacturing and service sectors (The TÜV Rheinland Group is a leading provider of technical services worldwide. Founded in 1872 and headquartered in Cologne, the Group employs more than 14,500 people in 500 locations in 61 countries and generates annual revenues of € 1.3 billion. The Group's mission and guiding principle is to achieve sustained development of safety and quality in order to meet the challenges arising from the interaction between man, technology and the environment.) AND **M/s Hologram Manufacturers Association of India (HoMAI),** an organization engaged in promoting the common interests of the Indian Hologram Industry (HoMAI is a registered, not-for-profit and a self-regulated national body of the carefully scrutinized and stringently chosen hologram manufacturers, who comply with certain conditions pertaining to their professional preparedness and proper manufacturing facilities and committed to the HoMAI Code for best business practice, respect for copyrights, high technical and security standards and to keep abreast of the latest technologies to stay ahead of the counterfeiters so that the hologram users could get the best anti-counterfeiting solutions and confidently rely on the HoMAI Members).

HSSMS

The Standard

The TUV Rheinland Hologram Safety and Security Management Standard (HSSMS) is built in the existing TUV R STAR ISMS platform partial rating which covers the entire implementation of best practices of information security management system considering the preservation of Confidentiality, Integrity and Availability against the related risk, threat & vulnerability obtained from the risk assessment within the scope of critical assets utilized by the organization for the core domain processes. This gives a clear picture that the standard will be a comprehensive and consolidated approach towards implementation of an effective security management system.

The TUV Rheinland Hologram Safety and Security Management Standard is a holistic standard which includes the following topics classified under different prevailing standards across the globe defining best practices for effective security process management.

- ISO 9001 (Quality Management System)
- ISO 27001 (Information Security Management System)
- ISO 28000 (Supply Chain Management)
- TUVR Brand Protection Platform
- DPA (Data Protection Act)
- PTP (Prototype Protection)
- BS25999 (Business Continuity Management)
- Intergraf
- HACCP
- BRC Global Standard

HSSMS

0.1 The Standard Committee

Sponsoring Organization – Hologram Manufacturers Association of India (HoMAI)

Developing Certification Body – TUV Rheinland (India) Pvt Ltd

External Consulting Organisation – Touchstone Assessment Consortium (TAC)

Governance Board

- HoMAI Board Members
- Managing Director, TUV Rheinland India
- Country Head – BRMS, TUV Rheinland India

The Standard Committee

Mr. C Ebenezer Bobson – Head – Standard Committee, TUVR
Mr. C R Parthasarathy – Principal Consultant, TAC
Ms. Mable Yuvaraj – Consultant, TAC
Mr. S Mohan Kumar – Auditor – TUVR

HSSMS

0.2 Copyright

- The TUVR-HoMAI Hologram Safety and Security Management Standard will be treated as joint property of both parties and neither party will be permitted to use these standards for any purpose or handover to any third party without the prior written permission of the other party.
- In addition to being privileged, confidential and a trade secret, all the content of these Standards, Logo, Trademark, and supporting documentation is owned by both TUVR & HoMAI jointly and will be protected by Indian Copyright laws. Both parties will not share, copy or use the written materials, images, trademarks, and/or logos without prior written authorization.
- All reports, documents, etc., exchanged between TUVR and HoMAI during the process of forming this standard and assessment / certification activities will remain the property of the party providing such documents.

HSSMS

0.3 Benefits of the Standard

- Identification of gaps and grey areas
- Effective Risk assessment for an organization as a whole
- Business continuity management practice implementation
- Disaster recovery process inlay
- Effective Incident management
- Effective Risk treatment
- Understanding and implementation of relevant security controls including the CWA requirements
- Establish good control over organizational shortcomings
- Improved Employee awareness and effective participation
- Effective response time
- Better visibility about Organizational risk
- Third party validation and market presence

HSSMS

0.4 Scope of the Standard

“Best practices of Hologram Safety & Security Management system considering the preservation of Confidentiality, Integrity and Availability against the related Risk, Threat & Vulnerability and the work and environmental safety related risk obtained from the organizational risk assessment process within the scope of critical assets utilized by the core domain processes.”

The Standard Logo

HoMAI
HSSMS
TÜVRheinland®
Precisely Right.

HSSMS

0.5 Standard Exclusions

“The standard does not cover the core domain process of manufacture of Holograms and related media. It confines itself solely to the risk management of confidentiality, integrity and availability considering safety & security across the process of manufacturing.”

HSSMS

HCSMS

0.6 Terminology

Access	Permission to approach, enter, speak with or use, admittance
Audit	Systematic, independent and documented process to obtain audit evidence to evaluate an objectivity to determine the extent to which criteria are fulfilled
Backup	Activity of copying files or databases so they will be preserved
Competency	Adequate possession of required skill, knowledge, qualification, capacity
Compliance	Act of complying in accordance with established guidelines, specifications or legislation
Control	Process operating with an acceptable range
Data	Collection of facts and figures that is organized so that it can be easily assessed, managed and updated
Disaster	An event occurring suddenly causing great loss of life, damage or hardship, Business failure
Discipline	A concerted or focused effort involving dedication of resources and risk which is directed to the accomplishment of a goal
Effectiveness	Extent to which planned activities are realized and planned results achieved
Equipment	Anything kept, furnished or provided for a specific purpose
Facilities	Something designed, built, installed to serve a specific function
HoMAI	Hologram Manufacturers Association of India
Hologram Safety and Security Management System	Management system to direct and control an organization with regard to safety and security of holograms
HSSM/R	Hologram Safety & Security Manager/Representative
Information	Knowledge communicated or received concerning a particular fact or circumstance, meaningful data
Integrity	Steadfast adherence to a strict moral or ethical code
Intruder	One who intrudes, thrusts himself or enters without right permission, a trespasser

Leakage	Something escaping or loss by leak
Legal	Meeting the requirement under law
Logical	Correct reasoning in accordance with principles
Logs	A record of everything that goes in and out of a particular process
Management	Coordinated activities to direct and control an organization
Mandatory	Required or commanded by authority, obligatory
Mitigation	Measures taken to limit the adverse effects of material or technological hazards
Organization	A group of people and facilities with an arrangement of responsibilities authorities and relationships
Outsource	Arrangement in which one company procures service or products from another company (outside supplier)
Procedure	Specified way to carry out an activity or a process
Process	A set of interrelated activities which transforms inputs to outputs
Protection	Preservation from harm, danger, injury
Property	Something tangible or intangible to which its owner has legal title
Regulatory	Legal and security compliance to law
Resources	System of facilities, equipment and services needed for the operation of an organization
Requirement	Need or expectation that is stated, generally implied or obligatory
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Risk	Probability of threat of a damage, injury, liability, loss or negative occurrence
Safety	Freedom from danger, quality of not causing injury or loss to any security equipment
Sample	A small representative portion of something
Security	Freedom from risk or danger, safety
Service	A deliverable
Service providers	A third party entity that manages and services of specific function of customer
Setting	The manner, position or direction in which something is set
Scrap	Discarded waste material

HSMS

Statutory	Requirement of standards set by the various state regulatory authorities
Sub contract	Practice of assigning part of the obligations and tasks under a contract to another company
System	Set of interrelated or interacting elements
TUVR	TUV Rheinland India Pvt Ltd
Validation	Confirmation through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled
Vulnerability	A weakness in a system that can result in harm to the system or its operations

HSSMS

Section 1 General Requirements

1.1 Hologram Safety and Security Management System

The organization shall establish, implement, operate, monitor, review, maintain and improve Hologram Safety and Security Management systems and identify, evaluate and implement corrective actions on all identified risks by periodical risk treatment method.

This Hologram Standard defines guidelines to support the interpretation, implementation and defined set of controls for managing Hologram Safety & Security and provides hologram safety & security best practice guidelines. By implementing this Standard, hologram organizations will be able to ensure a minimum requisite level of security that is appropriate to their organization's requirements and maintain the confidentiality, integrity and availability of hologram information from counterfeit.

This Hologram Standard applies to hologram manufactures in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand via fax, over computer networks or by post), as the information must always be appropriately protected.

1.1.1 Description of Hologram Manufacturing Processes (refer annexure B)

1.1.2 Interaction of Processes (refer annexure C)

1.2 Scope

1.2.1 Scope of Certification

The organization shall define the scope and boundaries of the HSSMS in terms of the nature of the business, the organization, its location, assets and technology and include details of and justification for any exclusion from the scope with prior approval from the Management.

The organization shall define an HSSMS policy that includes a framework for setting objectives and establish an overall sense of direction and principles for action with regard to Hologram Safety and Security taking into consideration, the business, legal, statutory and regulatory requirements aligned with risk treatment method conducted on all assets identified with prior approval from Management.

1.2.2 Applicable statutory and regulatory requirements

The Hologram standard specifies requirements needed to demonstrate its ability to consistently meet the applicable statutory, regulatory, and customer requirements.

HSSMS

1.3 Exclusions

1.3.1 Exclusion claims

When exclusions are made, claims of conformity to this standard are not acceptable, unless these exclusions do not affect the organization's ability or responsibility to provide product that meets customer and applicable statutory and regulatory requirements.
Excluded controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons.

1.3.2 Control of excluded processes

The exclusion of any process control shall provide the justification for their exclusion.

HSSMS

Section 2 Documentation Control

2.1 Hologram Safety and Security Manual

2.1.1 The hologram manufacturing organization shall have a manual exclusively developed for providing safety and security for hologram manufacturing.

2.1.2 The manual shall state the management commitment to Hologram Safety and Security in the form of a hologram safety and security policy and have a scope which addresses the requirement of this standard, including justification for any exclusion.

2.1.3 Requirements specified in the manual shall be fully implemented by the organization.

2.1.4 The Hologram Safety and Security manual shall be readily available to the identified persons in the organization as well as the customers, depending on contractual requirements.

2.2 Document Control Procedure

2.2.1 Documents required by the hologram safety and security system (HSSS) shall be controlled.

2.2.2 Documented procedure shall be established to define the following actions:

a) Approval of all documents developed, prior to its issue.

b) Review changes to current documents and update them, if necessary.

c) Current version of applicable documents is made available at all relevant points of use.

d) Documents are legible, identifiable and readily retrievable

e) Distribution of documents are controlled

f) Obsolete documents are removed from all points of use. They are preserved or disposed

2.2.3 The HSSM shall be responsible for control of documents

HSSMS

2.3 Mandatory Procedures

2.3.1 The organization shall establish the following procedures, implement, and also maintain the hologram safety and security processes as per the requirements of the relevant procedure.

2.3.2 Procedures required:

a) Control of documents

b) Control of records

c) Internal process audit

d) Management process review

e) Process of manufacturing

f) Access control

g) Risk management

h) Safety and security system evaluation

2.4 Operation Procedures

2.4.1 The organization shall develop relevant procedure/s to establish, implement and maintain the required safety and security system for the manufacture of hologram.

2.4.2 In addition, the procedure/s developed may contain details of work instructions/standard operating procedures.

HSSMS

2.5 Records Control

2.5.1 The organization shall ensure that records and data pertaining to hologram safety and security are effectively controlled.

2.5.2 The records shall be identified, stored, protected from un-authorized access.

2.5.3 Records shall be retrieved in a reasonable time and their retention period defined.

2.5.4 Documents shall be clearly legible, unambiguous.

2.5.5 Organization shall ensure the availability of current version of records at all points of use.

2.5.6 The electronic records shall be protected from loss, destruction, un-authorized change.

2.5.7 Any alteration in the record shall be appropriately authorized with justifications.

2.5.8 Obsolete records shall immediately be removed and preserved, disposed or otherwise, in accordance with the requirements of the organization.

2.6 Mandatory Records

2.6.1 The organization shall prepare a list of mandatory records, taking into consideration its various mandatory requirements.

2.6.2 To provide evidence for hologram safety and security, the mandatory records shall include:

a) Management review meeting agenda and minutes of meeting

b) Customer contract review

c) Customer approval for samples submitted

d) Customer feedback including complaints

2.3 Mandatory Procedures

2.3.1 The organization shall establish the following procedures, implement, and also maintain the hologram safety and security processes as per the requirements of the relevant procedure.

2.3.2 Procedures required:

a) Control of documents

b) Control of records

c) Internal process audit

d) Management process review

e) Process of manufacturing

f) Access control

g) Risk management

h) Safety and security system evaluation

2.4 Operation Procedures

2.4.1 The organization shall develop relevant procedure/s to establish, implement and maintain the required safety and security system for the manufacture of hologram.

2.4.2 In addition, the procedure/s developed may contain details of work instructions/standard operating procedures.

2.5 Records Control

2.5.1 The organization shall ensure that records and data pertaining to hologram safety and security are effectively controlled.

2.5.2 The records shall be identified, stored, protected from un-authorized access.

2.5.3 Records shall be retrieved in a reasonable time and their retention period defined.

2.5.4 Documents shall be clearly legible, unambiguous.

2.5.5 Organization shall ensure the availability of current version of records at all points of use.

2.5.6 The electronic records shall be protected from loss, destruction, un-authorized change.

2.5.7 Any alteration in the record shall be appropriately authorized with justifications.

2.5.8 Obsolete records shall immediately be removed and preserved, disposed or otherwise, in accordance with the requirements of the organization.

2.6 Mandatory Records

2.6.1 The organization shall prepare a list of mandatory records, taking into consideration its various mandatory requirements.

2.6.2 To provide evidence for hologram safety and security, the mandato ry records shall include:

a) Management review meeting agenda and minutes of meeting

b) Customer contract review

c) Customer approval for samples submitted

d) Customer feedback including complaints

HSSMS

e) Access control review record

f) System manager appointment

g) Incident and risk assessment report

h) Internal process audit findings

i) Scrap disposal (shims and process scrap)

j) Training and evaluation

k) Legal, statutory and regulatory requirements

l) External service provider agreement

2.7 Operation Records

2.7.1 The organization shall maintain records to demonstrate the effective control of its hologram safety and security process.

2.7.2 The records can be in any form (hard/soft copy) and shall be maintained in the relevant process area under the control of the process head.

2.7.3 The operation records shall include

a) Visitor’s entry/exit including visitor’s pass

b) Process logs

c) Strong room records for entry and exit

d) Strong room for receipt, issue and removal of items stored

e) CCTV monitoring

f) Hologram equipment maintenance including repair and installation

g) Security equipment location

h) Material movement for processed and scrap items

i) Service provider, transporter evaluation and rating

j) Compliance

k) Validation

l) Packing and dispatch

HSSMS

Section 3 Management Control

3.1 Management Commitment

3.1.1 Hologram safety and security management system (HSSMS)

a) The management shall be responsible for effective implementation and maintenance of HSSMS

b) Effective implementation shall be evidenced by defining the scope of HSSMS and deploying the required resources administered by a security administrator as a responsible manager in providing the required support for implementing security policy, security objectives, procedures, incident and risk management, compliance to statutory and regulatory requirements, and commitment to meet customer security requirements.

c) Evidence of periodical reviews.

3.1.2 Improvement of the safety and security system

a) The organization shall continually improve the hologram safety and security management system to enhance customer satisfaction

b) Areas of improvement can be identified by one or more of the following ways:

1) Suggestions from process operators

2) Feedback from customers

3) Internal process audit findings

c) Management in consultation with the HSSM shall review and make decisions for incorporating the necessary changes to the security system.

3.1.3 Statutory and regulatory requirements

The products manufactured by the organization shall meet the legal, statutory and regulatory requirements of security, including that of customer

3.1.4 Integrity of system due to change management

a) The organization shall ensure the integrity of hologram safety and security management system, whenever changes are planned and implemented.

b) Customer approval obtained for changes in the security system, where necessary.

3.1.5 Hologram Safety and Security Manager/Representative (HSSM/R)

Management shall appoint a senior employee, holding executive position/function, of its organization as the HSSM/R

The responsibilities and authorities of the HSSM/R in addition to his current duties are clearly defined in the following ways:

a) Establish, implement and maintain a hologram safety and security management system as per this standard

b) Create and promote awareness of the system throughout the organization including service providers, wherever safety and security of holograms is involved

HSSMS

c) Report to the management for the effective functioning of the hologram safety and security management system

d) Liaison with customers, regulatory agencies

3.2 Management Responsibility

3.2.1 Safety and security policy

a) Management formulates a safety and security policy in line with its business requirements, with the intent of enhancing customer confidence.

b) The safety and security policy shall state the intentions of the organization to meet its customer and regulatory obligations

3.2.2 Business objectives

Management shall ensure

a) Continuous business activity by timely decisions

b) Events for interruptions are defined

c) Risk assessment

3.2.3 Management commitment

a) Management shall show its commitment within the organization by establishing the safety and security management system.

b) Effectiveness and continual improvement of the system ensured.

3.2.4 Approval / review

a) The safety and security policy developed by the organization shall be approved by the Management and approved security policy displayed in all process areas.

b) Security policy is reviewed and evaluated during the management review meetings.

c) Changes suggested and discussed during the management review meetings are incorporated into the system.

d) Changes introduced in the policy communicated to the relevant personnel including service providers.

3.2.5 Awareness of safety and security policy

a) The management shall ensure the awareness of the safety and security policy and also its customer security requirements to all personnel dealing with hologram safety and security throughout the organization including service providers.

b) Awareness includes safety and security education, adequate training.

3.3 Safety and Security Objectives

3.3.1 Customer requirements

a) Management ensures top priority for customer requirements of safety and security while formulating the security objectives.

HSSMS

b) The objectives shall be measurable and reviewed during management review meetings for their effectiveness.

3.3.2 Organization requirements

a) Management assesses its own safety and security requirements including legal, statutory and regulatory while formulating the safety and security objectives.
b) The objectives shall be measurable and reviewed during management review meetings for their effectiveness.

3.4 Hologram Process Resource Management

3.4.1 Resource identification

All information (safety and security) processing resources of the organization shall be clearly identified.

3.4.2 Resource maintenance

All organizational resources shall have periodic maintenance plan and execution.

3.4.3 Resource owner nomination

Information and information processing resources identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and safety and security of the resources.

3.4.4 Inventory

All identified organization's safety and security assets shall be drawn up and maintained as inventory. Regular review of the asset inventory shall be defined and controlled.

3.4.5 Hologram safety and security asset protection

All identified organization assets shall be protected against risk, threat, theft, damage & vulnerabilities.

Protection measures shall include:

a) Employees responsibilities

b) Review for periodic maintenance

c) Effective physical control of customer property

d) Asset registers review at planned intervals.

e) Incident report including necessary corrective action.

3.4.6 Utility services protection

Management shall implement effective ways to protect the utility equipment within organization.

All utility equipment shall have regular maintenance checkups and the reports of maintenance shall be reviewed by management responsibilities.

HSSMS

3.4.7 Asset handling

Rules for the acceptable use of hologram safety and security assets shall be clearly identified, documented and implemented

3.4.8 Return of assets

All organization's hologram safety and security assets used by employees, contractors and third party users shall be returned during transfer or termination of the employee / contract agreement.

3.5 Human Resources & Training

The organization shall ensure that relevant employees having direct/indirect bearing on the Hologram Safety and Security understand their responsibilities and are competent for the roles they are assigned in order to minimize risk of theft, misuse of safety and security facilities.

HSSMS

3.5.1 Personnel confidentiality / induction / screening

a) Hologram Safety and Security responsibilities are addressed to the employees prior to their induction.

b) Confidentiality of safety and security measures considered during screening of employee.

c) Personnel confidentiality declaration obtained from employee after induction.

d) Certificate of conduct maintained for each employee.

3.5.2 Security & safety training

a) Hologram Safety and Security aspects are appropriately addressed during training.

b) Awareness of safety and security policy and their objectives are addressed during training.

c) Awareness of safety and security of service providers is ensured during contractual agreement.

3.5.3 Personnel / Organisation property

a) Provision for locker facilities to store personal belongings of employees/visitors outside the process areas made.

b) Hologram Safety and Security equipment should not be taken off site without prior permission.

c) Storage media, sensitive data and licensed software prevented from unauthorised access.

3.5.4 Disciplinary action

a) Disciplinary or appropriate action initiated against employees who break rules and regulations.

b) Disciplinary or appropriate action taken against service providers for infringement of service rules.

3.5.5 Security passes

a) Security passes issued to visitors upon entering the premises and surrendered to the security at the exit gate at the completion of their visit.

b) Employees provided with security passes and displayed on person during working hours.

c) Service providers provided with security passes and displayed on person during working hours.

3.5.6 Responsibility and competency

The organization shall define the responsibility and competency of its personnel having direct bearing on the safety and security of the holograms manufactured.

The following activities should be considered while defining the responsibility and competency:

a) Sales and service

b) Procurement

c) Design and development

d) Production facilities

e) Verification

f) Regulatory compliance

g) Internal audit

h) Service provider

3.5.7 Access rights & removal

a) Zonal or perimeter access to employees, service providers and visitors indicated in their security passes to prevent un-authorised access

b) All relevant personnel should know the scope of their permitted access (Prominent and legible display signs indicating access limits and boundaries for restricted entry).

c) User access rights shall be reviewed at regular intervals.

d) The organization shall ensure against misuse of access facilities of employees and service providers. Access rights immediately removed for unauthorised intruders and appropriate actions initiated.

3.6 Customer Requirement

3.6.1 Review of requirement

The organization shall review the requirements related to the safety and security requirements of Hologram product in addition to commercial requirements. This review shall be conducted prior to the organization commitment to supply a Hologram product to customer.

Records of the respective review results shall be maintained and reviewed in each processes of the product.

3.6.2 Customer approval

A prior approval for the developed samples shall be obtained from customer requirement.

When there is a change in the customer requirement of safety and security during any stage of the process, it shall require formal approval from customer.

3.6.3 Statutory and regulatory requirement

The review of product requirement shall take into consideration statutory and regulatory requirements.

HSSMS

3.6.4 Changes to contract

A formal review mechanism shall be defined and the same initiated when there is a change in customer requirement. Records of the review shall be maintained.

Information regarding the changes shall immediately be communicated to relevant personnel in the organization.

3.6.5 Feedback / complaint

The organization shall define and implement effective measures for customer complaints & feedback.

3.6.6 Customer notification / information

All customer notification / information in the form of feedback / complaints shall be recorded as incidents, and it shall be discussed with the management before necessary corrections and corrective actions are initiated.

3.7 Procurement Management

3.7.1 Supplier evaluation / monitoring

The organization shall ensure that the purchased product conforms to specified purchase requirements. The organization shall evaluate and select the supplier based on their ability to satisfy customer requirement. Supplier performance shall be reviewed periodically. Records of the review shall be maintained.

3.7.2 Service provider (security/transport) evaluation

The organization shall evaluate the ability of service providers for providing security during handling, transporting and exchanging of interim/final product located inside/outside organization premises periodically.

Records of the review shall be maintained.

3.7.3 Supplier rating

Review output of supplier performance shall assign a rating based on performance with regard to product quality, customer requirements, statutory & legal requirements and other product based requirements. Supplier rating shall be evaluated and necessary action shall be initiated based on the rating.

3.8 Risk Management

3.8.1 Process-related risk management

The organization shall establish risk assessment methodology for its hologram manufacturing that meets the organization's contractual, legal & regulatory requirements, and it shall be executed at planned intervals.

Records of risk assessment shall be maintained.

HSSMS

3.8.2 Product-related risk management

The organization shall evaluate and conduct product related safety and security risk assessment in each stage of process, and effective measures shall be established to control the impact to product during production covering all stages of design to delivery.

3.8.3 Criteria for acceptance

Management shall evaluate and approve

a) Risk assessment methodology

b) Criteria for accepting risk identified

c) Acceptable level of risk

3.8.4 Risk treatment

Management shall evaluate the risk calculation and define the suitable method of risk assessment. The identified risk will be categorized with respect to acceptable level of risk. Unacceptable risks are evaluated and appropriate corrective actions initiated.

Records of risk treatment plan shall be maintained.

3.9 Incident management

Management shall establish responsibilities and procedures for recording response and implementation of corrective actions to the incident at the process level.

3.9.1 Incident report

Hologram manufacturing events and weakness shall be reported through effective channels and such records shall be maintained as evidence.

The responsibilities assigned by management shall include the investigation & review of incident occurred.

3.9.2 Corrective / preventive action

The reported incident shall be discussed with management and necessary Corrective / Preventive actions initiated.

3.9.3 Analysis

Management and management representatives will

a) Involve in analyzing the incident recorded

b) Take the necessary Corrective / Preventive action

c) Discuss on mechanism to quantify the value & volume of incidents

3.9.4 Review of incident

All incidents can be recorded and ranked with type and severity in nature.

HSSMS

Recorded incident will be reviewed with management and management responsibilities as and when the incident is recorded.

3.10 Internal Process Audits

3.10.1 Scope

a) The organization shall define and conduct internal process audits at planned intervals to determine whether the Hologram Safety and Security Management systems are effectively implemented across the organization's scope.

b) Internal process audits shall be planned well in advance taking into consideration the status and importance of processes, areas to be audited, and results of previous audits.

c) The audit criteria, scope, periodicity and methods shall be defined.

d) Selection of auditors shall ensure that the personnel responsible have undergone regular internal auditor training in order to conduct the audit with objectivity and impartiality.

e) Auditors shall not audit their own process during the internal process audit.

f) Documented procedure shall be established to define the responsibilities and requirements for planning and conducting audits.

g) Records of audits and their results shall be maintained and reviewed.

h) Management shall ensure necessary corrections, correction & corrective action on audits outcome without undue delay.

i) Follow-up action shall be initiated to ensure that corrective actions are implemented, and reviewed for effectiveness.

3.10.2 Auditor training / competency

Organization shall provide necessary training to selected employees to carry out internal process audits within the organization.

Management shall ensure that administrator/management representative gets the adequate training in order to control the effectiveness of Hologram Safety and Security Management System within the organization.

3.10.3 Audit records

Records of audits and their results shall be maintained and reviewed

3.11 Management Process Review

3.11.1 Frequency of review

Management shall review the Hologram Safety and Security Management System at planned intervals to ensure the effectiveness and suitability of HSSMS.

The frequency of Management process review shall be defined in a procedure, and the execution shall meet the requirements

3.11.2 Agenda for meeting

Management process review shall consider the following during the review:

HSSMS

a. Internal process audit reports
b. Previous management process review output
c. Safety and security incidents
d. Status of corrective and preventive action
e. Risk assessment report
f. Any changes that could affect the HSSMS
g. Customer feedback, recommendations for improvement

3.11.3 Review output approval, execution, and communication

Management shall document decisions and actions on improvement on HSSMS

3.11.4 Review records

Review records of management process review shall be established and maintained to provide evidence of management review process discussion.

HSSMS

Section 4 Physical Controls

4.1 Isolation and Secured Areas

4.1.1 Identification of critical and sensitive areas

Management shall identify critical and sensitive process and areas to ensure effective control on physical security.

It shall be reviewed at regular intervals for identifying the critical and sensitive areas.

4.1.2 Defining sensitive perimeters within the process

The identified sensitive and critical areas within the process and organization shall be controlled from unauthorised access to Hologram Manufacturing location.

Perimeters like walls, access-controlled entry and exit gates, manned reception desks, physical security guards shall be assigned to protect such sensitive areas.

Critical sensitive areas such as Design, Master shooting and electroforming process shall be protected by appropriate entry control to ensure that only authorised personnel are allowed access.

Security perimeter shall be implemented to protect areas that require security level.

All personnel, vehicles shall be checked upon entering or leaving organization boundary.

4.1.3 Physical barriers to prevent unauthorised entry/exit

Sensitive areas shall be protected by appropriate entry / exit controls to ensure that only authorised personnel are allowed access.

Sensitive/Critical process may be separated by walls, access-controlled entry, Biometric gates and manned reception to prevent unauthorised personnel entry

Management shall appoint (or assign responsibility to) process owners to ensure control over entry/exit of unauthorised personnel within their process areas.

4.1.4 Physical security protection

Physical security guards shall be placed strategically throughout the organization.

Physical security guards shall be provided with appropriate training on security checks and handling emergency situations.

Management shall implement effective physical security checks on personnel to safeguard the product and its sensitive customer information

Physical security may be implemented to ensure effective control on movement of products during the process and final stage.

4.1.5 Additional barriers

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.

Physical control implemented to ensure business continuity during such scenarios.

HSSMS

4.1.6 Vehicle movements

Management shall develop a policy on all vehicle inspection against various risk, threats and vulnerabilities

a) All vehicles shall have identification process method

b) Parking of vehicle will be separated against organization level and outsiders (supplier, third party vendors, and service providers)

c) Strict guidelines will be prepared and approved by management on physical checking

d) Details of vehicle and drivers shall be maintained, and it shall be produced if any verification required and it should be approved by management

e) A formal process for vehicle movement shall be recorded

f) Record of vehicle movement shall be recorded and reviewed

4.2 Physical Access Control

4.2.1 Entry/departure of visitors

Management shall define and implement effective means of control and physical verification of visitors at entry and exit points.

4.2.2 Authorised access area to visitors

Management shall have process to control visitors to restricted access areas.

Management shall ensure that visitors are accompanied by authorized personnel to the restricted access areas.

Management shall approve by a formal process the entry of visitors to restricted areas.

All employees, visitors, contractors and third party vendors shall be screened as per the access control policy.

4.2.3 Visible identification for employees, visitors, service providers and suppliers

a) Management shall develop and implement a procedure to control unauthorised access within the organization.

b) All employees, visitors, contractors, service providers and suppliers shall be identified by unique identification process (such as ID card, Access cards) to have control over access to organization premises.

c) Management responsibilities shall review the tracking system to ensure effective physical movement of employees, contractors, and supplier and service providers.

4.2.4 Review of physical access control

Management shall develop and maintain a formal process to ensure access control for authorised personnel.

Management shall review the access control at planned intervals to ensure authorized shall get access to their own process and unauthorised location shall be denied

HSSMS

Section 5 Production Security Control

5.1 Access Control

5.1.1 Customer information management

The organization shall develop a process to understand the requirements of its customers. Impact of the interruptions and incidents on the business continuity shall be considered.

The following processes should be considered:

a) Samples developed by design and development, shall be approved by the customer, and limited samples preserved for reference.

b) Risk in Hologram safety and security shall be considered while reviewing the customer requirements

c) Plans to be developed to restore the regular process after interruptions and incidents.

d) Customer specific security procedures to be developed depending on contractual obligations.

e) Guidelines for customer verification of their product and connected security should be developed.

5.1.2 Logical access control

The organization shall take effective steps to prevent unauthorised access to sensitive / critical process areas.

5.1.2.1 Design and Development

a) Data received from customer securely preserved in the design and development process.

b) Access to customer data, computer software restricted to authorised users.

c) Logs maintained for receipt of data, samples developed and communication with master shooting process.

d) Management shall ensure effective control over design transfer.

5.1.2.2 IT Network Management

a) The organization shall prevent un-authorised access to IT network systems.

b) Effective control shall be exercised during transmission of information.

c) User's connectivity to the network shall be restricted depending on the business requirements.

d) Unique user ID and password system shall be enforced.

5.1.3 User Identification and Access

The organization shall ensure unique identification for the employees and contractors and generic identification for visitors and customers.

a) Unique identification applicable to operation personnel and service providers.

b) Traceability to user ID shall be established.

c) Generic identification provided for customers and visitors where necessary.

HSMS

5.2 Security Planning

The organization shall plan and operate the security system to meet the current and projected requirements of the customer.

5.2.1 Customer requirement

a) Customer requirements reviewed to ensure the availability of resources.

b) Adequacy of hologram manufacturing security risk considered for existing system based on projected customer requirements

5.2.2 Subcontracting for security

a) Assess the adequacy of the current security facility including service providers.

b) Make provision for additional security requirements to meet the projected demand of security system due to increased capacity requirement planned.

c) Evaluate the adequacy of service providers responsible for providing additional security personnel.

5.2.3 Surveillance checks

a) Assess the adequacy of the current surveillance checks for Hologram safety and security.

b) Make changes to the current surveillance system in order to meet future capacity requirements identified.

c) Additional surveillance checks planned, tested and approved prior to their regular use.

5.2.4 Disaster management

The management shall be responsible for reducing the risk in Hologram Safety and Security. Adequate and appropriate information and evidence regarding security breach, vulnerabilities and violations shall be obtained.

Vulnerabilities/violations in Hologram safety and security should cover

a) Operation and monitoring of security equipment

b) Implementation and maintenance of relevant procedures in processing facilities

c) Adequacy of service providers

d) Access control to employees, service providers and visitors

e) Scrap management in process, strong room and disposal areas

f) Resolution of customer complaints

g) Incident management for security failures and review of evidence

h) Maintenance of security logs

i) Confidentiality of personnel involved in Hologram Safety and Security

j) Integrity of security management system

k) Security weakness

The organization shall analyze and improve relevant security process with regard to the above vulnerabilities/violations.

HSSMS

5.3 Scrap Management

The organization shall ensure minimum risk during handling of scrap in process facilities, strong room and disposal areas. Applicable legal, statutory and regulatory requirements shall be considered. A procedure shall be established for management of scrap.

5.3.1 Identification and storage of setting/process scrap

a) Scrap generated during machine setting shall be identified and stored in process areas. System shall minimize the accumulation of waste in process areas.

b) Scrap generated during regular machine operation shall be identified and stored in process areas

c) Setting and process scraps mixed according to the convenience

d) Appropriate logs maintained for scrap

e) Adequate security for storage of scrap ensured in process area

5.3.2 Movement of scrap

a) Movement of process scrap to strong room from process facilities ensured under secured conditions

b) Logs maintained for transport of scrap to strong room and disposal area`

c) Accumulated scrap moved to disposal area under secured conditions

d) Authorised personnel and service providers accompany scrap to strong room and disposal area

5.3.3 Storage of scrap

a) Stored in process and strong room; ensured against theft, misuse and destruction

b) Authorised personnel identified for handling of scrap; un-authorised access to scrap prevented

c) Logs maintained for receipt, storage and movement of scrap

d) Logs stored securely

5.3.4 Scrap disposal/Destruction as per customer and legal requirements

a) Destruction or disposal of waste material shall prevent misuse and misappropriation

b) Periodicity of disposal shall be defined

c) Appropriate methods of disposal shall be employed (burning or shredding)

d) Disposal of scrap is witnessed by authorised personnel

e) Records maintained for disposal shall be certified by authorised personnel

f) The organization shall take effective measures for disposal of scrap if internal facilities are not available

5.4 Internal Processing

The organization shall effectively manage Hologram safety and security throughout the manufacturing facilities. Customer requirement of safety and security for its products during manufacture should be the prime consideration in addition to regulatory requirements. Inputs and outputs of Hologram manufacturing process to be controlled.

HSSMS

5.4.1 Unauthorised access/immobilisation

a) The organization shall ensure single point entry to its manufacturing facilities. This includes movement of raw material, semi and finished products

b) Packing and storage areas secured

c) Hologram manufacturing facilities safeguarded from break-ins and sudden/surprise attacks

5.4.2 Spot check on employees & service providers

a) Spot or surprise checks performed on employees and service providers to prevent unauthorised removal of semi/finished products from the process areas.

b) Verification shall be conducted at regular intervals.

c) Disciplinary or appropriate action initiated against employees and service providers breaking rules and regulations.

5.4.3 Intruder detection

a) Activation and deactivation of Hologram safety and security equipment restricted to authorised personnel

b) Intruder detection constantly monitored by CCTV in process areas including packing and dispatch

c) Daily back up of CCTV recordings taken and maintained outside the premises

d) Hologram safety and security system made known to authorised and restricted personnel including service providers

5.4.4 Access to security equipment

a) Access to Hologram safety and security equipment during installation, operation and repair shall be controlled

b) Access to security equipments restricted to authorised personnel

c) Disciplinary action initiated for breach of access to security equipments

d) Removal of equipment for repair shall be authorized

e) CCTV cameras installed strategically in risk areas and their operations monitored

5.4.5 Protection of security equipment including software/backups

a) Personnel handling security equipments and related I.T. systems shall be competent

b) Security of equipment and I.T. systems handled by authorized personnel

c) Security equipments protected from theft, destruction, unauthorized tamper during and after working hours

d) Sensitive safety and security system employed in design and master sheeting isolated

e) Design and master sheeting software stored in dedicated computers

HSSMS

5.4.6 Removal of property

a) Design information, customer approved samples Hologram safety and security equipment and hologram products (semi and finished) shall not be taken outside the premises without authorization

b) Security equipment removed from the premises for repair shall be authorised

c) Surprise checks conducted to prevent unauthorised removal of property

5.4.7 Risk identification and mitigation

a) Management shall apply appropriate safety and security controls throughout the hologram manufacturing facility to reduce risk

b) Risk level requested by the customer shall be considered while planning for Hologram safety and security

c) Risk assessment carried out periodically and safety and security controls reviewed

d) Risk evaluation/assessment carried out whenever significant changes in Hologram safety and security planned and implemented

e) Risk identified from design to delivery to the end user and appropriate controls installed

5.4.8 Incident management and reporting

a) The organization shall ensure effective management of incidents, whenever un-foreseen events, breach of Hologram safety and security including weaknesses in security occurs

b) Timely corrections, corrective and preventive actions shall be ensured

c) An incident report prepared by system administrator as quickly as possible after the incident has occurred.

d) The incident report will include root cause analysis, corrections, proposed corrective and preventive actions.

e) The incident report will be reviewed by the Management and after their approval, customer is notified.

f) The incident report will be discussed during the management review meeting

g) Records of incidents, notification to customer and review will be maintained by system administrator

5.4.9 Safety and security information vulnerability

a) The organization shall assess/evaluate the vulnerability of its safety and security information communicated to unauthorised personnel

b) Risk associated with vulnerability shall be monitored

c) Actions initiated to prevent Hologram Safety and Security risks in vulnerable areas

HSSMS

Section 6 Production Safety Control

6.1 Safety System Facilities (equipment, personnel, logs)

6.1.1 Safety of equipments

a) Management shall ensure safety of equipment and product against theft / damage

b) The organization shall ensure that the safety of Hologram security equipments is not jeopardized during installation, processing and maintenance operations

c) During temporary repair or shut down, safety of the equipments ensured

d) Necessary physical security guards shall be provided to protect all equipment and product

e) A maintenance programme covering all the security equipments shall be established and implemented

f) Service agreement prepared when maintenance services are outsourced

g) Computers in which confidential data is stored are secured and unauthorised access prevented

h) Hologram safety equipment prevented against unauthorised operation during and after work hours

i) Semi-finished and finished products shall be protected against tampering, counterfeiting, theft and damage

j) Hologram manufacturing processes and its security equipments protected from intruders

k) Hologram safety equipments automatically switched on/off during/after working hours

l) Process for regular maintenance of equipment shall be developed, maintained and reviewed

6.1.2 Safety of personnel

a) Safety of process personnel, service providers and visitors ensured

b) Personnel protected from physical and environmental factors

c) Operational personnel provided with safety wear (hand gloves, face mask, etc.,)

d) Designated changing facilities provided for all personnel: whether operators, visitors, contractors before entering the process facilities

e) Protective gear

1) Where work wear (hand gloves, mask and goggles) required, employees shall be provided with suitable protective equipment

2) Appropriate changing facilities shall be provided

3) Toilets shall be adequately segregated from manufacturing facilities

4) In high risk operations (master sheeting), personnel shall be provided with overalls, headwear and footwear

6.1.3 Logs

a) Process logs, maintenance records and security monitoring data shall be protected and controlled

b) Access to Hologram manufacturing and security logs shall be controlled

c) Sensitive data in design and master sheeting protected from environmental effects

HSSMS

d) Responsible personnel for maintenance of logs shall be identified

e) Appropriate measures established to prevent leakage of information

f) Backup data for security monitoring equipment stored outside the premises and periodically tested for its effectiveness

g) Hologram safety and security related logs maintained by HSSM including installation and repair

h) Appropriate log books maintained in Hologram manufacturing facilities and their safety and security controlled

i) Management shall develop a procedure to control movement of semi-finished, finished products and employees within organization

j) Log/register recording on user activities, movement of personnel/semi & finished products shall be produced for better tracking of product status

k) Log shall be prepared and kept maintained for an agreed period to assist in future investigation on tracking of products/incidents root cause. Such logs shall be protected against tampering and unauthorised access

6.2 Packing, storage, dispatch and loading areas for products and in-process items including protection of in-process, finished products and scrap

6.2.1 In-process items and finished products protected from product mix-up, theft and destruction

6.2.2 Safe areas identified for process items before final packing

6.2.3 Access to strong room facility

a) Storage of films, semi finished, finished items and scrap shall be readily identifiable and controlled

b) Logs maintained for entry and removal of items

c) Logs maintained for entry/exit of personnel

d) Logs maintained for scrap stored and destroyed

6.2.4 Transfer point control

a) Supplier, service providers and contract employees shall be protected to prevent unauthorized access to process areas

b) Supplied items, semi finished & finished products shall be transferred within organization, and it shall be controlled by effective physical checking

c) No items are transferred without necessary approvals from management

d) Management shall define a dedicated point for transferring materials/products from or to organization

e) Such transfer point shall be verified at regular intervals and reporting of security weakness shall be recorded as incidents

HSSMS

6.2.5 Dispatch and loading

a) Dispatch and loading operations shall be controlled

b) Supervision during dispatch and loading ensured

c) Authorised personnel shall certify the consignment before dispatch

d) Dispatch and loading of consignment takes place in secured areas.

e) Customer informed regarding consignment dispatch before the operations

f) Status of vehicle movement monitored till delivery to customer

g) Limited access to authorized personnel only during loading of the consignment

6.2.6 Storage area segregation

Production, packing and storage areas shall be adequately segregated

6.3 Emergency Management

a) Management ensures safety and security of personnel, security equipment, service providers and visitors.

b) Deviation from the mandatory and operation procedures of this standard including customer requirements deemed as emergency issues

c) Emergency issues for the safety and security of equipment and personnel resolved immediately

d) Deviation from legal, statutory and regulatory requirements shall be prevented and controlled

6.3.1 Surprise attacks

The organization shall ensure the safety and security of the personnel, equipments during surprise attacks

HSSMS

Section 7 Verification and Validation Control

7.1 Verification

7.1.1 Safety and security equipments

The organization ensures the verification of its safety and security equipments during/after installation, operation and after repair

Verification by competent personnel carried out at appropriate stages of Hologram manufacture at frequent intervals to ensure:

a) Verification carried out by competent personnel

b) Safety and security equipments are operating as per the requirement of the relevant procedure

c) Safety and security monitoring equipment is working effectively

d) Corrective and preventive action taken to resolve non conformities

e) Customer verification due to contractual obligations

f) Maintenance of verification logs

g) Authorization for dispatch

7.1.2 Calibration of safety and security equipment

The organization shall determine the calibration of security equipment at frequent intervals in a controlled manner in order to provide evidence that all security equipment is performing as per required specifications

Security equipment shall be

a) adjusted and re-adjusted where necessary

b) identified for calibration status where necessary

c) protected from unauthorised adjustments

d) periodically checked to confirm the ability of the computer software used in design and master shooting

7.1.3 Safety and security records

The organization shall verify appropriate security records, which provide evidence that security equipments are performing as per required specifications.

The records that need to be verified are:

a) CCTV camera for process monitoring

b) Employee/visitor access

c) Calibration of equipment

d) In-process and final scrap

e) Scrap disposal

f) Disposal of damaged/ un-used films and plates

g) Loading and dispatch of finished products

h) Strong room operations

HSSMS

i) Customer-approved samples

j) Backup data

7.2 Validation

7.2.1 General

The organization shall validate new safety and security equipments during installation and after repair in order to ensure the compatibility of the entire Hologram safety and security system.

7.2.2 Equipment

Safety and security equipment shall be validated for:

a) access for installation, adjustment, repair and replacement

b) monitoring function

c) immobilisation during/after working hours

7.2.3 Methods and logs

Methods employed in Hologram manufacturing facilities regarding security shall be validated,

Methods and logs validated are:

a) Standard operation procedures or work instructions developed for effective operation of security equipment

b) Standard operation procedures or work instructions are authorized

c) Current version available at points of use

d) Safety and Security logs for raw materials, process area access, entry / exit of visitors

7.2.4 System safety and security internal/external

The organization shall validate the Hologram safety and security system provided to prevent un-authorised access and control.

Validation methods used are:

a) Internal/external safety and security meets customer and regulatory requirements

b) Adequacy of safety and security system

c) Risk management

7.2.5 Personnel qualification internal

The organization shall qualify employees to ensure the Hologram safety and security system is effectively functioning.

Validation methods used are:

a) Personnel confidentiality declaration

b) Personal references for new recruits

c) Personnel security training

d) Spot checks on personnel

HSSMS

e) Employee security passes

f) Evaluation for service providers

HSSMS

Section 8 Compliance Management

8.1 Legal, statutory and regulatory requirements

a) The organization shall comply with all legal, statutory and regulatory requirements

b) The organization’s control and responsibilities for each of the requirements shall be defined

c) Appropriate records to be maintained

8.2 Customer Requirements

a) Customer requests, tenders and contracts shall be reviewed

b) To ensure customer requirements for Hologram safety and security during process and dispatch

c) Samples developed shall be approved by the customer, identified and retained

Amendments or changes to customer requirements shall be reviewed and communicated to relevant functions

8.3 Internal Process Audit

a) The organization shall plan and implement internal audits of its Hologram safety and security systems and procedures to ensure they are effective

b) The audit shall be scheduled periodically and the scope of audit defined

c) The scope shall take into consideration the risk associated with that process

d) Internal audit carried out by identified trained personnel of the organization.

e) Independence of the auditor from auditing his/her own process ensured

f) Process owners to implement corrective and preventive actions based on results of audits.

g) Follow up audits scheduled ensure implementation of corrections, corrective and preventive actions

h) Records of the audit maintained by the HSSM

8.4 Customer Data Protection

a) The organization shall ensure the safety and security of the customer property

b) Customer property is identified, verified, protected and safeguarded during all stages of manufacturing and storage

8.5 Safety and Security Policy

a) Security policy communicated to all relevant personnel having a bearing on the security of holograms manufactured

b) Safety and security policy approved by the management

c) Safety and security policy displayed in the relevant process areas where security of hologram is involved

d) Safety and security policy is reviewed during management meeting for its effectiveness

HSSMS

8.6 Safety and Security Procedures

a) Compliance to mandatory and operation procedures verified during internal process audit

b) Effectiveness of procedures verified during internal process audit

c) Surprise checks conducted to verify adherence to procedures

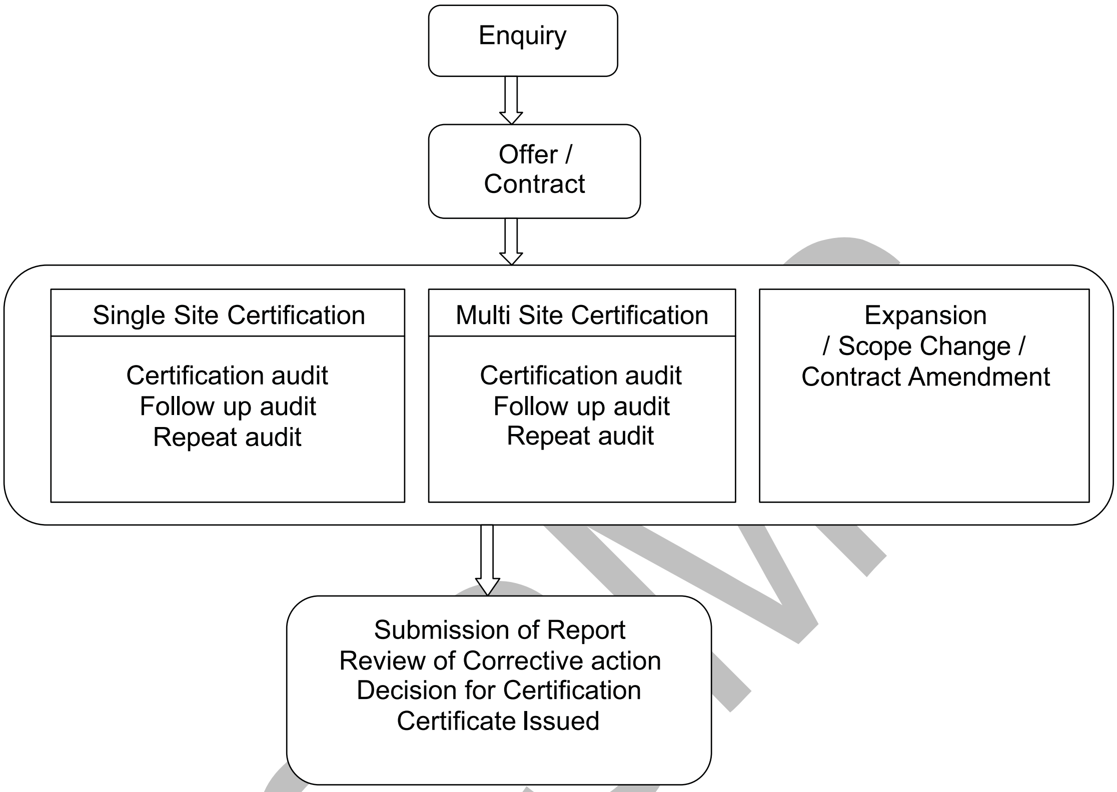
8.7 Safety and Security Records

a) Management shall comply with mandatory and operations records verified during internal process audit

b) Identification, retrievability and retention of the records shall be verified

HSSMS

Annex A – Audit Methodology



Enquiry

Offer / Contract

Single Site Certification

Certification audit
Follow up audit
Repeat audit

Multi Site Certification

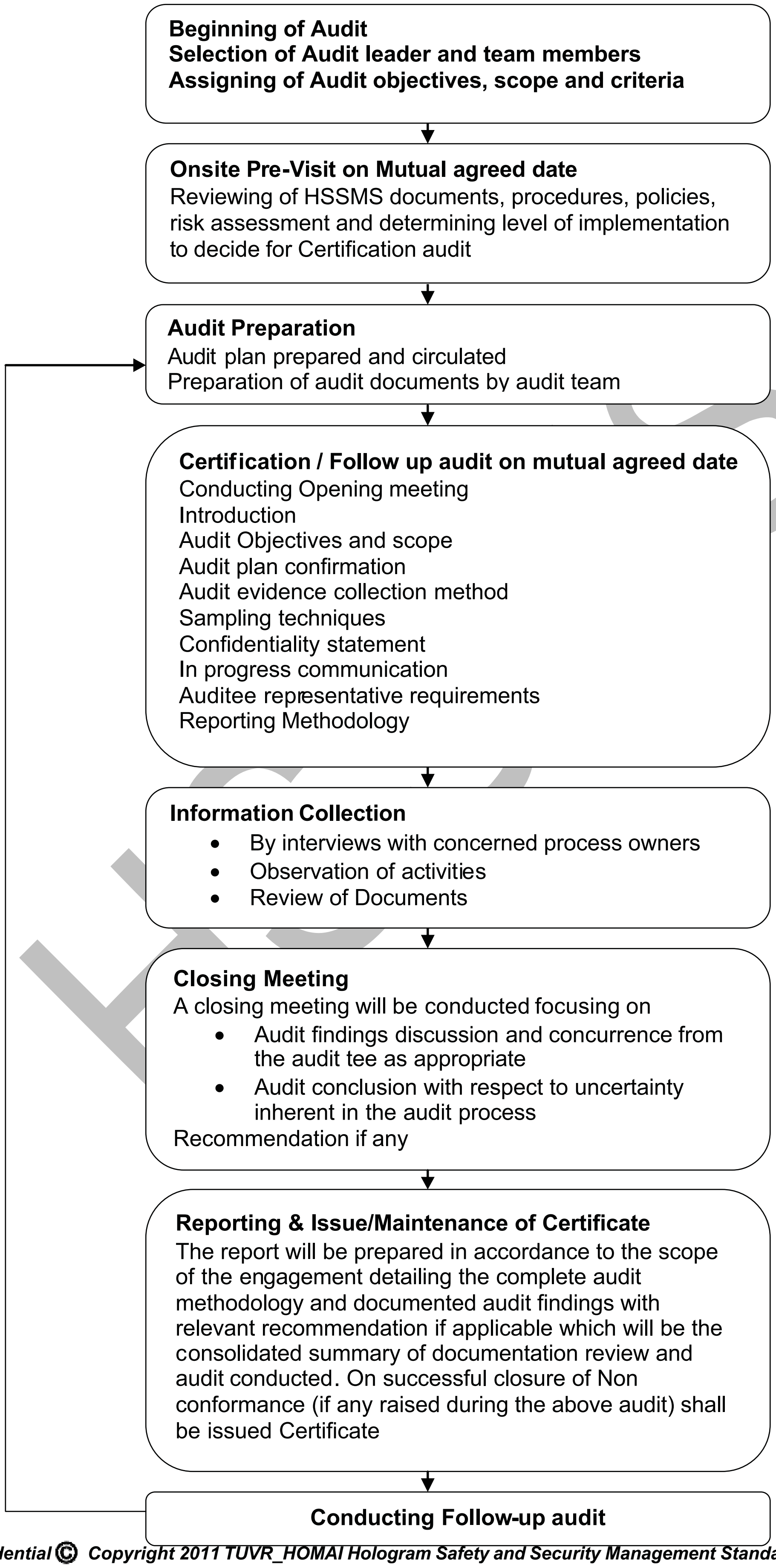
Certification audit
Follow up audit
Repeat audit

Expansion / Scope Change / Contract Amendment

Submission of Report
Review of Corrective action
Decision for Certification
Certificate Issued

HSOM

Annex A - Audit Methodology (cont….)



Beginning of Audit
Selection of Audit leader and team members
Assigning of Audit objectives, scope and criteria

Onsite Pre-Visit on Mutual agreed date
Reviewing of HSSMS documents, procedures, policies, risk assessment and determining level of implementation to decide for Certification audit

Audit Preparation
Audit plan prepared and circulated
Preparation of audit documents by audit team

Certification / Follow up audit on mutual agreed date
Conducting Opening meeting
Introduction
Audit Objectives and scope
Audit plan confirmation
Audit evidence collection method
Sampling techniques
Confidentiality statement
In progress communication
Auditee representative requirements
Reporting Methodology

Information Collection

- By interviews with concerned process owners
- Observation of activities
- Review of Documents

Closing Meeting
A closing meeting will be conducted focusing on

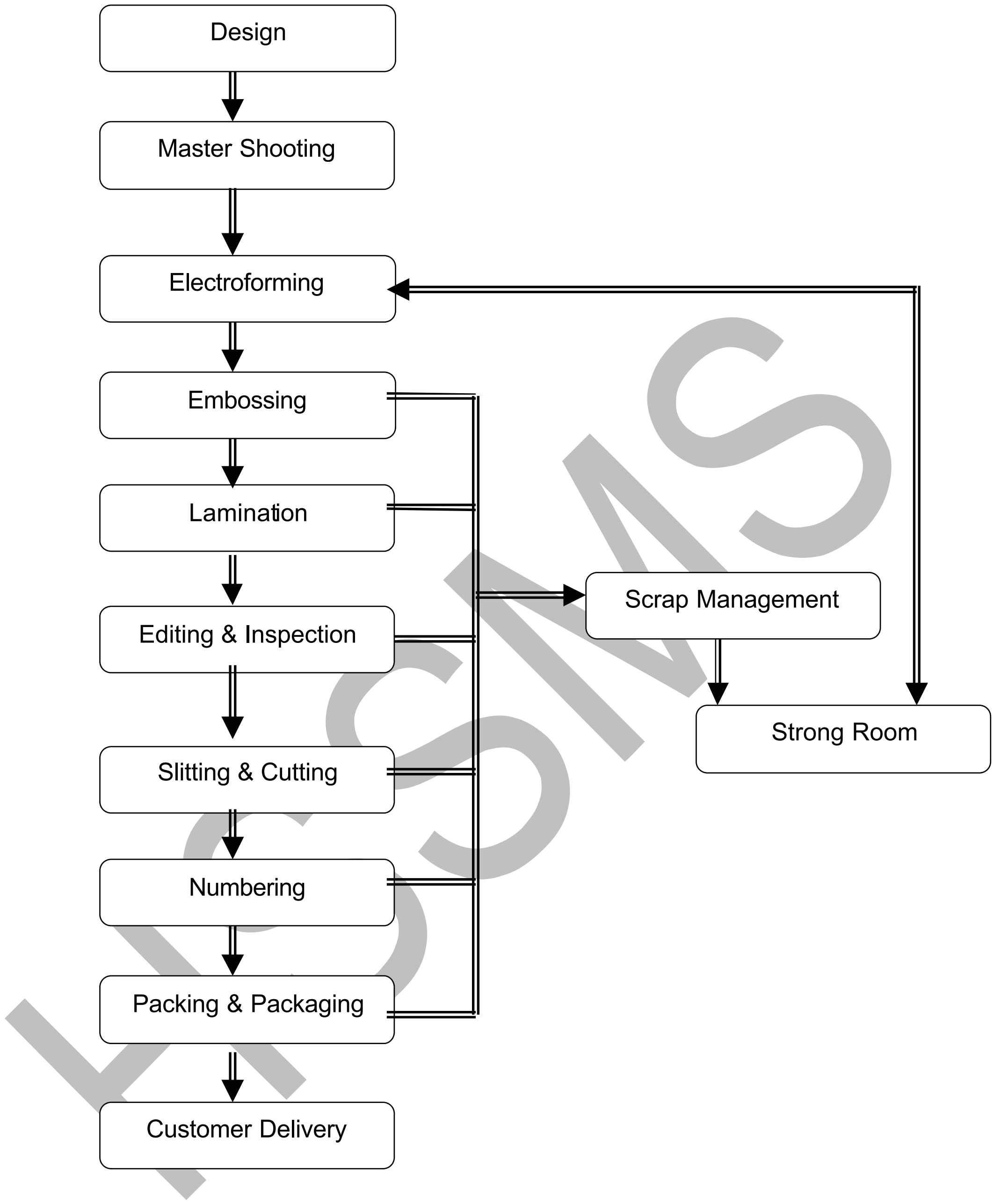
- Audit findings discussion and concurrence from the audit tee as appropriate
- Audit conclusion with respect to uncertainty inherent in the audit process

Recommendation if any

Reporting & Issue/Maintenance of Certificate
The report will be prepared in accordance to the scope of the engagement detailing the complete audit methodology and documented audit findings with relevant recommendation if applicable which will be the consolidated summary of documentation review and audit conducted. On successful closure of Non conformance (if any raised during the above audit) shall be issued Certificate

Conducting Follow-up audit

Annex B - Process Flow Chart



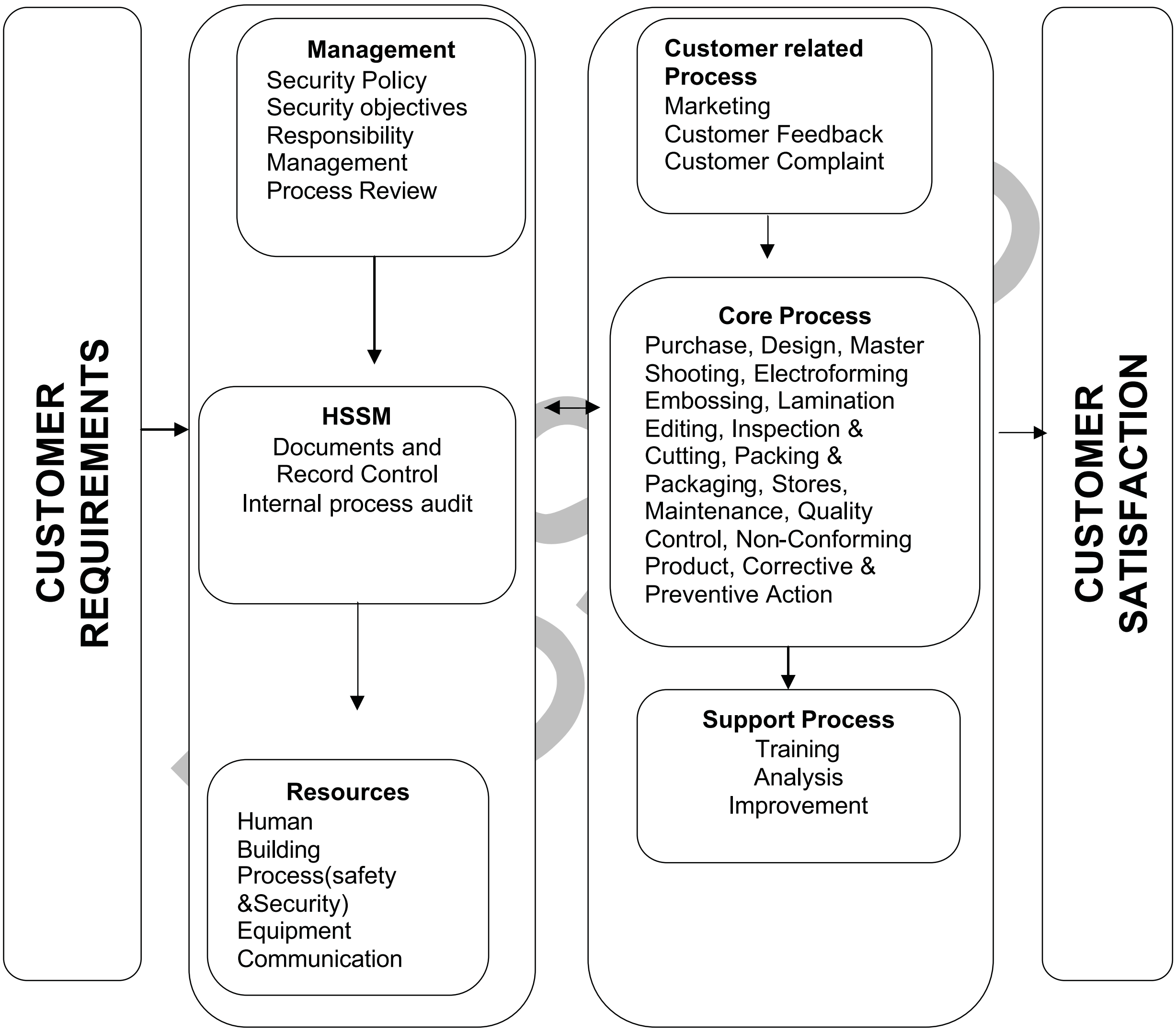
HSSMS

Annex B - Description of Processes (Cont....)

Process	Input	Output
Design	Information received from Marketing and Customers	Design of Hologram as per customer requirement in Designing software
Master Shooting	Softcopy of Customer approved Hologram design	Transfer of Hologram image into Glass plate using 2D/3D, Dot Matrix & Laser technique
Electro Forming	Final approved Hologram in Glass plate	Conversion of Glass plate image into Nickel Plate using electrical analysis
Embossing	Nickel Plate	Embossed with Polyester Film Material
Lamination	Printing Polyester Film Material	Laminated with release paper using Adhesives in roll & flat form
Editing & Inspection	Laminated Hologram product in Roll and Flat forms	Screened and approved
Slitting & Cutting	Final product after editing and inspection	Cutting as per customer requirement
Numbering/Marking	Semi Finished product after inspection and cutting	Numbering as per customer requirement by Laser, Ink Jet technologies for identifying the hologram & improving the security features
Packing & Packaging	Finished Product	All finished products shall be identified with customer & product information and it shall be packed as per customer requirement

HSSMS

Annex C - Interaction & Control of Processes



HSSMS

For more information, contact
Hologram Manufacturers Association of India (HOMAI)
21, Ground Floor, Devika Tower 6,
Nehru Place, New Delhi 110019, India
Tel: +91.11. 4161 7369
Email:info@homai.org
Website: www.homai.org

About HOMAI

Founded in 1998, The Hologram Manufacturers Association of India (HOMAI) is an industry body of manufacturers and suppliers of holographic OVD’s and its allied products in India. Since its inception, it has been encouraging its members to adopt best practices, standards and usage of advance technology in providing cost effective solution against counterfeiting. It is a trusted source for market and technology consultancy for anti-counterfeiting industry, brand protection and product enhancement in India.