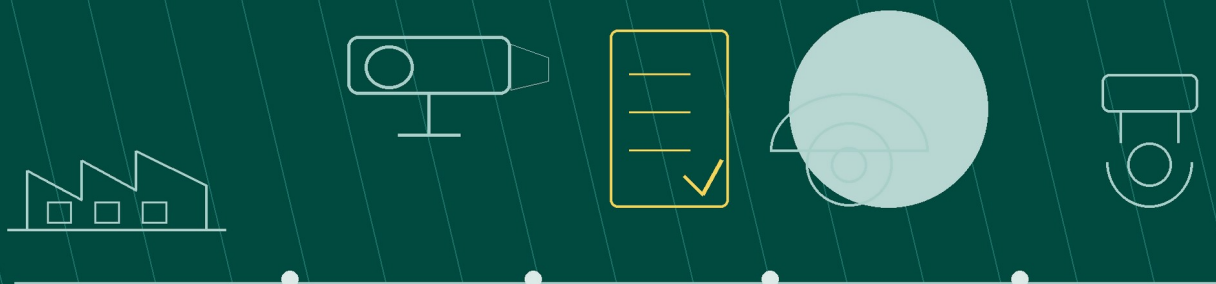


ACTi

Physical Security End-to-End Solution Provider

White Paper | STQC Ready Product Service

STQC READY PRODUCT SERVICE



A practical white paper for planning STQC-ready surveillance products, local assembly, certification support, secure system integration, and deployment in India

Contents

- 1** Executive Summary
- 2** About ACTi Corporation
- 3** Definition of "STQC Ready Product Service"
- 4** Core Technical Concepts
- 5** High-Value Applications
- 6** System Architecture
- 7** ACTi Product Portfolio Overview
- 8** Related Keywords and Terminology

Document purpose

This white paper explains ACTi's STQC Ready Product Service, the difference between product readiness and certification, the technical and project controls that support formal evaluation, and the way OEM or semi-knocked-down (SKD) options can be integrated into an India-focused surveillance program.

It is written for system integrators, consultants, security managers, procurement teams, local surveillance brands, manufacturers, and end users that need a durable framework for government, public-sector, critical-infrastructure, enterprise, and large-scale video-surveillance projects in India.

The document uses product types, form factors, and general categories rather than model names so it can remain useful as individual products and generations change.

Reading guide

Use Sections 3 and 4 to define the readiness and compliance workstream, Section 5 to map business and deployment value, Section 6 to align certification scope with system architecture, and Section 7 to select durable product categories without locking the white paper to a specific part number.

1. Executive Summary

STQC Ready Product Service is a structured product-preparation and certification-support offering for surveillance projects in India. ACTi describes the service as covering camera categories that can be prepared toward India's Standardisation Testing and Quality Certification (STQC) requirements, with OEM and SKD partnership options. The stated readiness areas include physical and hardware security, access control, firmware integrity, cybersecurity features, power safety, and environmental reliability. [1]

The service is valuable because certification readiness is not only a datasheet attribute. A successful program must control the exact hardware, firmware, configuration, documentation, testing inputs, local assembly process, facility inspection, application administration, and post-certification change process. ACTi's published workflow includes commercial scope definition, product preparation, internal verification, formal laboratory testing, facility inspections, customer-led application administration, and official certificate publication. [1]

For system integrators and consultants, this means translating tender language into a traceable bill of materials, tested configuration, secure system design, installation standard, and evidence package. For end users, it means procuring a solution whose certification scope, lifecycle support, cybersecurity posture, recording architecture, and operational controls are understood before deployment.

Core message

STQC readiness is a controlled process, not a marketing label.

Treat the camera category, hardware revision, firmware build, cybersecurity settings, test evidence, assembly method, inspection scope, application responsibility, and deployed system architecture as one governed project.

Key takeaways

- STQC-ready and STQC-certified are not interchangeable terms; certification is completed only through the applicable formal process and official publication.
- Product selection should be based on the use case and required form factor, then frozen into a testable and traceable configuration.
- Hardware security, access control, firmware integrity, cybersecurity, safety, and environmental reliability must be considered together.
- OEM and SKD options can support local branding and local assembly objectives, but commercial, technical, labeling, and regulatory responsibilities must be defined in writing.
- A certified device still needs secure network design, recording, operator permissions, time synchronization, maintenance, and change control at system level.
- Before tender submission, confirm the latest eligible categories, certification grouping possibilities, laboratory scope, lead time, NRE, minimum order conditions, and regional requirements with ACTi.

Procurement principle

Do not specify only "STQC-compliant camera." Specify the required certification status, applicant/brand owner, exact device category, hardware and firmware identity, local assembly scope, test and inspection responsibilities, evidence package, system integration, lifecycle change-control process, and acceptance criteria.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. ACTi states that it has more than 20 years of security-industry experience and has been a pioneer in video-based security technology development and innovation. [5]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem includes video surveillance cameras, recording and video-management platforms, access control, central management, system health management, AI-enabled technologies, mobile operation, and third-party integration. [5]

This broader scope matters for STQC-focused projects. Product readiness and certification activities must remain connected to the deployed solution: secure camera configuration, reliable recording, network protection, operator permissions, event handling, evidence export, and lifecycle support all influence the security value of the final system.

Why ACTi is relevant to STQC-ready projects

ACTi strength	Project relevance
End-to-end system scope	Camera categories, Windows-based NVR/VMS, central monitoring, access control, AI, and system health can be planned as one architecture rather than isolated products.
Product preparation workflow	ACTi publishes a step-by-step service path covering scope, commercial terms, product preparation, internal verification, formal lab testing, facility inspection, and certification publication. [1]
OEM and SKD options	Branding, packaging, firmware interface, settings, mechanical/electrical customization, and levels of local assembly can be defined according to the selected service type. [2][3]
Security and reliability focus	ACTi identifies firmware integrity, cybersecurity, hardware security, power safety, and environmental reliability as central STQC readiness areas. [1]
Project lifecycle support	System integration, device management, recording, redundancy, health monitoring, and technical support help keep the deployed solution aligned with its intended security outcome. [5]

3. Definition of "STQC Ready Product Service"

STQC Ready Product Service is an ACTi offering that helps customers select suitable surveillance product categories, define a commercial and technical scope, prepare the selected hardware and firmware configuration, perform readiness verification, coordinate formal laboratory testing, support required facility inspections, and proceed toward customer-administered certification in India. [1]

STQC stands for Standardisation Testing and Quality Certification. STQC is an attached office of India's Ministry of Electronics and Information Technology and provides testing, calibration, certification, IT and e-governance, and capacity-building services through laboratories and centres across India. [4]

For surveillance products, ACTi highlights essential requirement areas such as physical and hardware security, access control, firmware integrity, cybersecurity features, power safety, and environmental reliability. ACTi also states that the certification is often mandatory for government tenders or public-sector deployments in India. [1]

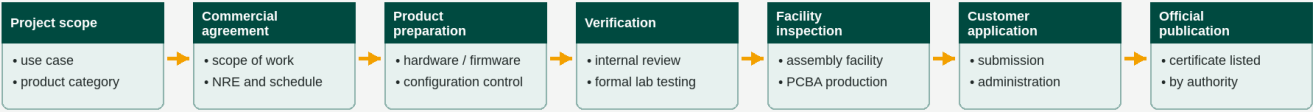
STQC-ready vs. related concepts

Term	Meaning	Common misunderstanding
STQC-ready product	A selected product category and configuration prepared to enter the defined verification, testing, inspection, and application process.	Readiness is not itself the final certificate and should not be presented as automatic certification.
STQC-certified product	A product/configuration that has completed the applicable evaluation and has an officially published certification status.	Certification scope may be tied to a specific brand, applicant, hardware/firmware version, facility, or product family.
OEM service	A branding/customization framework that may range from ACTi-branded project naming to unbranded or customer-branded products. [3]	A logo change alone does not establish certification, local-content status, or responsibility for technical changes.
SKD service	A semi-knocked-down supply arrangement in which defined final assembly steps are completed by the customer under an assembly procedure. [2]	Local assembly must be controlled; waterproofing, labeling, inspection, and quality responsibilities vary by service type.
System compliance	The broader secure deployment of cameras, network, storage, VMS, accounts, logging, maintenance, and operating procedures.	A certified device does not automatically make the complete installed system secure or compliant.

Visual concept

From STQC-ready preparation to published certification

The readiness service supports a controlled product, evidence, testing, inspection, and application workflow.



ACTi support focus: category selection, scope definition, product preparation, verification support, and lab coordination

Key boundary: "STQC-ready" is not the same as "STQC-certified." Certification depends on the agreed configuration, formal evaluation, inspections, customer administration, and official publication.

Design note

The practical value of the service comes from traceability. The project team should be able to identify which product category was selected, which hardware and firmware were evaluated, which documents were submitted, where assembly occurred, which facility was inspected, who administered the application, and what was ultimately published.

Practical deployment interpretation

For a government, smart-city, transport, utility, campus, or enterprise project, the tender may require both product certification and a secure deployed system. The system integrator should therefore keep the certification workstream synchronized with network design, recording, cybersecurity hardening, installation quality, acceptance testing, and maintenance.

4. Core Technical Concepts

STQC-ready product planning should begin with the tender requirement and the deployment risk, then move toward a controlled product and evidence scope. The following concepts help project teams avoid selecting a camera category that appears suitable commercially but cannot be traced, tested, assembled, deployed, or maintained consistently.

Concept	Practical meaning
Readiness vs. certification	Use precise language. Readiness describes preparation and capability to enter the process; certification describes a completed, officially recognized outcome for a defined scope.
Essential requirement domains	Confirm physical/hardware security, access control, firmware integrity, cybersecurity, power safety, and environmental reliability requirements for the target evaluation. [1]
Configuration control	Freeze and identify hardware revision, firmware build, enabled services, default settings, credentials policy, cryptographic options, and test configuration.
Evidence and documentation	Maintain specifications, declarations, software/firmware records, test inputs, assembly procedures, labeling, traceability records, and corrective-action evidence.
Formal testing and inspection	Plan for laboratory evaluation and the inspection of relevant customer assembly and manufacturer production facilities as required by the application process. [1]
OEM / SKD scope	Define branding, model naming, UI branding, packaging, settings, assembly work, quality checks, and responsibility for any design or firmware change. [2][3]
Group certification strategy	Where permitted, consider whether related form factors or configurations can be grouped, while preserving clear boundaries for differences that affect testing or security.
Lifecycle change management	Assess whether component, firmware, supplier, assembly, labeling, or feature changes require review, regression testing, notification, or certification updates.
System-level cybersecurity	Use segmentation, least privilege, secure remote access, time synchronization, logging, patch governance, backup, and incident response beyond the device itself.

Specification interpretation

A technically capable camera can still fail the project if the tested configuration is not the one shipped, firmware changes are uncontrolled, assembly records are incomplete, the applicant role is unclear, or the installed network exposes unnecessary services. Conversely, a governed readiness program can reduce tender risk, accelerate technical review, and create a defensible chain from product selection to field deployment.

Readiness capability matrix

Use this matrix during tender review, product selection, and scope negotiation. Each project requirement should be translated into a controlled product attribute, evidence item, responsible party, and acceptance output.

Project challenge	What can go wrong	Capabilities / controls to specify	Expected output
Ambiguous certification language	Readiness is presented as certification or the applicant/brand scope is unclear.	Define terminology, certificate status, applicant, brand, category, and official verification method.	Accurate tender response
Uncontrolled firmware	The tested build differs from the delivered or updated build.	Version identification, integrity controls, release approval, rollback, change log, and update policy.	Traceable firmware baseline
Hardware or supplier change	A component change affects security, safety, reliability, or test results.	Revision control, approved component list, impact assessment, regression testing, and notification path.	Controlled hardware identity
Local assembly variation	Assembly quality, sealing, labeling, or records differ by facility or operator.	Assembly SOP, training, tools, environmental controls, inspection, serialization, and nonconformance handling.	Repeatable production evidence
Fragmented documents	Evidence is distributed across sales, engineering, factory, lab, and customer teams.	Named document owner, controlled repository, revision index, submission checklist, and retention policy.	Complete evidence package
Secure device, weak system	Certified devices are deployed on flat networks or with weak credentials and unmanaged access.	VLANs, least privilege, secure protocols, firewall rules, time sync, logging, VMS permissions, and maintenance SOP.	Secure operational architecture

How to use this matrix

For tender writing, define the certification requirement first. Then specify the eligible product category, exact tested configuration, branding and local-assembly scope, required documentation, laboratory and inspection responsibilities, application ownership, deployed system architecture, cybersecurity controls, acceptance tests, and lifecycle change process.

Important project control

Any substitution after proposal approval - including firmware, image sensor, system-on-chip, memory, network interface, enclosure, power component, manufacturing site, or local assembly step - should be assessed against the certification and tender scope before deployment.

5. High-Value Applications

STQC Ready Product Service is most valuable where formal product assurance, cybersecurity expectations, public procurement, local branding, local assembly, and large-scale surveillance deployment overlap. The service can help project teams create a more controlled path from tender specification to tested product and operational system.

Application	Operational value	Typical environments
Government and public-sector tenders	Supports accurate certification language, controlled product selection, evidence preparation, and reduced risk of proposing an ineligible configuration.	Government buildings, municipal projects, public agencies
Smart city and city surveillance	Creates a repeatable product baseline for large fleets while aligning camera categories, network security, recording, and lifecycle support.	Roads, public spaces, command centres, urban infrastructure
Transportation infrastructure	Helps define ruggedness, cybersecurity, firmware control, long-distance imaging, and centralized evidence requirements.	Rail, metro, airports, ports, highways, depots
Critical infrastructure and utilities	Supports stronger assurance for restricted sites where device integrity and reliable evidence are essential.	Power, water, oil and gas, telecom, data centres
Education and healthcare	Provides structured procurement for campuses and public facilities that need accountable surveillance and controlled access.	Schools, universities, hospitals, laboratories
Industrial and enterprise projects	Combines secure device procurement with OEM/SKD, local service, central monitoring, and operational change control.	Factories, warehouses, offices, logistics sites
India-based surveillance brands	Enables partners to evaluate branding, customization, assembly, testing, and certification responsibilities for a local portfolio.	OEM brands, distributors, manufacturers, solution providers

Value by stakeholder

Stakeholder	Main benefit
System integrator	A clearer path to tender compliance, product traceability, secure architecture, and acceptance documentation.
Consultant	More precise specification language for certification status, evidence, testing, local assembly, system security, and lifecycle control.
End user / security manager	Greater confidence that the purchased product category and deployed configuration match the intended assurance scope.
Local brand / manufacturer	A structured OEM or SKD framework for branding, assembly, product preparation, testing support, and certification planning.
Procurement team	A more defensible buying decision based on official status, scope, lifecycle risk, support, and total project responsibility.

6. System Architecture

An STQC-ready project should be designed as two synchronized architectures: the operational video-surveillance system and the readiness/certification workstream. The field device, network, recording platform, operator workflow, and maintenance model must match the security objective, while the tested product identity, evidence package, facility scope, application, and lifecycle controls remain traceable.

Reference architecture for an STQC-ready surveillance solution

Device readiness and certification workstream must remain aligned with the deployed video system.



Parallel readiness and certification workstream



Design question: can the exact tested configuration be traced from the field device to the evidence package and certification scope?

Architecture layers

Layer	Role in an STQC-ready surveillance solution
Field layer	Camera form factor, mounting, optics, lighting, environmental exposure, power, local storage, tamper risk, and physical installation quality.
Device security layer	Accounts, access control, firmware integrity, secure configuration, service exposure, cryptographic options, logs, and update governance.
Network layer	PoE, switching, VLANs, firewalls, secure management, remote access, time synchronization, bandwidth, resilience, and monitoring.
Recording and management layer	Windows-based NVR/VMS, live view, recording, retention, playback, search, export, user permissions, central monitoring, and health status.
Compliance workstream	Product/configuration identity, documentation, testing, facility inspection, application administration, publication, and change control.
Operations layer	Operator SOP, alarm response, incident handling, evidence export, account review, backup, maintenance, patching, and audit trail.

Architecture warning

Certification of a device does not replace secure system engineering. Flat networks, weak passwords, exposed remote services, inaccurate time, missing logs, incorrect recording profiles, uncontrolled updates, or untrained operators can undermine the value of a certified product.

7. ACTi Product Portfolio Overview

ACTi presents the STQC Ready Product Service around a broad surveillance portfolio and complementary recording software. To keep this white paper durable, the categories below describe product types and use-case roles rather than individual model numbers. The exact eligible products, specifications, firmware, regional availability, and certification grouping should be confirmed for each project. [1]

Portfolio categories

Category	Where it fits	Use-case fit
Fixed bullet cameras	Directional outdoor or indoor views where a visible, easy-to-aim form factor is preferred.	Perimeters, roads, gates, building exteriors
Zoom bullet cameras	Scenes that need field-adjustable framing or longer-range identification.	Transport, utilities, campuses, critical sites
Fixed dome cameras	Low-profile, vandal-resistant viewing for public or semi-public areas.	Entrances, corridors, stations, offices
Zoom dome cameras	Protected form factor with installation-time or operational framing flexibility.	Lobbies, platforms, warehouses, public facilities
PTZ cameras	Active monitoring, optical zoom, patrols, and wide-area response.	City surveillance, ports, roads, large campuses
Hemispheric and multi-imager cameras	Wide-area situational awareness with fewer mounting points.	Intersections, halls, concourses, open facilities
Special-environment cameras	Enhanced protection for corrosive, hazardous, or demanding sites.	Coastal, chemical, industrial, explosive-risk areas
Windows-based NVR/VMS platform	Recording, live monitoring, playback, scalable storage, integration, and cybersecurity controls.	Control rooms, multi-site systems, evidence management
OEM and SKD services	Branding, customization, local assembly options, and project-specific commercial/technical scope.	India-based brands, manufacturers, distributors

Portfolio-level capabilities to confirm

- Required form factor, resolution class, lens type, low-light and WDR performance, IR range, frame rate, audio, I/O, local storage, analytics, environmental protection, and vandal resistance.
- Firmware integrity, authentication, authorization, secure protocols, logging, update method, default-service policy, password policy, and configuration export/restore.
- Recorder/VMS compatibility, stream profiles, retention, failover, search, evidence export, user permissions, central management, and system health monitoring.
- OEM/SKD branding, labeling, packaging, UI customization, assembly procedure, tooling, quality inspection, serialization, warranty, and corrective-action process.
- Certification status, applicant/brand scope, hardware and firmware identity, test-lab scope, inspection requirements, documentation, lead time, and change-control obligations.

Project note

Confirm the latest eligible product categories, detailed specifications, certification scope, accessory compatibility, firmware baseline, recorder compatibility, and regional commercial terms from current ACTi documents before project submission.

8. Related Keywords and Terminology

The following keyword reference groups collect common terms related to STQC readiness, surveillance product certification, secure camera design, OEM/SKD programs, local assembly, system architecture, and project procurement.

Core topic keywords

STQC Ready Product Service, STQC-ready cameras, surveillance product readiness, India CCTV certification, video surveillance certification support, security camera compliance, public-sector surveillance procurement

STQC and certification keywords

Standardisation Testing and Quality Certification, MeitY, essential requirements, certified product, certification scope, formal laboratory testing, facility inspection, certificate publication, certification application

Product category keywords

fixed bullet camera, zoom bullet camera, fixed dome camera, zoom dome camera, PTZ camera, hemispheric camera, multi-imager camera, anti-corrosion camera, explosion-protected camera

Hardware and firmware security keywords

physical security, hardware security, firmware integrity, secure boot, signed firmware, firmware version control, configuration baseline, hardware revision, tamper resistance, secure update

Cybersecurity and network keywords

access control, authentication, authorization, least privilege, HTTPS, TLS, VLAN, firewall, secure remote access, time synchronization, audit log, vulnerability management, password policy

Testing and documentation keywords

test evidence, compliance matrix, product traceability, bill of materials, technical file, assembly SOP, inspection record, revision control, corrective action, test report, submission checklist

OEM, SKD, and local assembly keywords

OEM camera service, white-label surveillance camera, unbranded camera, custom branding, semi-knocked-down camera, local assembly, Made in India planning, assembly facility inspection, PCBA production facility

Video and analytics keywords

high-resolution surveillance, optical zoom, infrared illumination, low-light camera, WDR camera, high-frame-rate video, people detection, vehicle detection, classification, recognition, edge analytics

System integration keywords

Windows NVR, video management system, live monitoring, playback, evidence export, centralized monitoring, scalable storage, multi-site surveillance, system health management, third-party camera integration

Applications and tender keywords

government CCTV tender, smart city surveillance, transport security, critical infrastructure surveillance, utility security, campus surveillance, public safety cameras, India surveillance project

Procurement and project keywords

STQC camera specification, certification verification, eligible product category, NRE, minimum order quantity, lead time, group certification, product change control, lifecycle compliance, tender acceptance criteria

Common question phrases

what is STQC Ready Product Service, what is the difference between STQC-ready and STQC-certified, how to select STQC-ready cameras for an India tender, how to verify an STQC certificate, what surveillance camera categories can be prepared for STQC, how does firmware integrity affect camera certification, how to manage hardware and firmware changes after certification, how does OEM branding affect certification scope, how does SKD local assembly support India projects, what documents are required for surveillance product testing, how are camera assembly facilities inspected, how to design a secure network for certified cameras, how to integrate STQC-ready cameras with an NVR or VMS, how to write an STQC camera specification, how to control product substitutions in a government CCTV tender

Source notes

Ref.	Source
[1]	ACTi Corporation, "STQC Ready Product Service," official product/service page. Accessed: July 16, 2026.
[2]	ACTi Corporation, "Semi-Knocked Down Products Service," official service page. Accessed: July 16, 2026.
[3]	ACTi Corporation, "OEM Service," official service page. Accessed: July 16, 2026.
[4]	Standardisation Testing and Quality Certification Directorate, Government of India, official website and organization overview. Accessed: July 16, 2026.
[5]	ACTi Corporation, "About ACTi," official corporate page. Accessed: July 16, 2026.

Revision note

This document is a marketing and technical education white paper. It is not an STQC certificate, legal opinion, tender approval, cybersecurity audit, electrical design, environmental test report, local-content determination, or final project design. Requirements and eligible product categories may change. Always verify current official requirements, certificate records, applicant/brand scope, test reports, hardware and firmware identity, facility obligations, labeling, local assembly, cybersecurity configuration, and tender conditions before submission or deployment.

Prepared by ACTi Corporation

For STQC-ready projects, confirm the target product categories, certification strategy, OEM/SKD scope, firmware and hardware baseline, documentation, testing, facility inspection, application responsibilities, system architecture, commercial terms, and regional availability with your ACTi sales contact or authorized system integrator.

sales@acti.com | www.acti.com