FEBRUARY 28, 2026

CREATIVA SECURITY CONSULTING – BUSINESS PLAN

A UNIFIED, LAWFUL, AND CIVILIAN SECURITY PLATFORM DELIVERING COMPLIANT, SCALABLE PROTECTION ACROSS THE CREATIVA ECOSYSTEM.

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Creativa Security Consulting – Business Plan

Business Plan and Institutional Charter
A Subsidiary of Creativa Center AB
Part of the Creativa Center Universe (CCU)

Version: 2026 Draft – Restricted Internal Use
Legal Form: Aktiebolag (AB)
Ownership: 100% Creativa Center AB
Jurisdiction: Sweden (EU), with operational corridors in EU/EUOS and Africa (COMESA, EAC, SADC)

EXECUTIVE SUMMARY

Creativa Security Consulting AB ("the Company") is established as the formal, licensed security subsidiary of Creativa Center AB, operating within the structural, ethical, and institutional architecture of the Creativa Center Universe (CCU). Its mandate spans protection, safeguarding, operational continuity, and lawful commercial security services. The Company exists to ensure that Creativa Center's rapidly expanding operations—including EUOS properties, ECHO infrastructure deployments, international missions under SFPSEI, and CCU executive activities—are protected by a coherent, legally compliant, professional, and ethically governed security capacity.

The Company forms one half of a dual-layer security architecture. The first layer, the Creativa Protective Security Unit, provides internal, non-commercial protective services for executives, staff, youth residents, properties, and operations. The second layer, represented by the Company, provides licensed commercial security services to Creativa entities and selected third parties. This dual structure ensures compliance with Swedish and international law, mitigates liability, preserves governance integrity, and enables long-term institutional credibility across all CCU initiatives.

The establishment of EUOS as a multi-property societal model for education, inclusion, and youth development requires a safeguarding environment that exceeds the general Swedish security market standards. Simultaneously, the deployment of high-value ECHO modules, the activation of African operations under SFPSEI, and the movement of senior officials in fragile or semi-fragile contexts necessitate a cross-continental risk doctrine and a structured partnership model with licensed local security providers.

Creativa Security Consulting AB will begin operations with a focused mandate: protecting Creativa's own properties, assets, personnel, and operational corridors, while gradually expanding into a selective commercial portfolio aligned with the Creativa ethos. The objective is not to mirror large, volume-based security actors such as Securitas or Avarn but to establish a high-integrity, high-standards security firm capable of supporting CCU's long-term institutional missions. Commercial growth is permitted but subordinated to ethical, legal, and reputational considerations.

The Company therefore serves two fundamental purposes:

1. To safeguard the operational integrity of Creativa Center's global mission.
2. To build a scalable, professional, and mission-aligned security architecture that supports EUOS, ECHO, and CCU's long-term international vision.

CHAPTER 1 — INSTITUTIONAL POSITIONING WITHIN THE CREATIVA CENTER UNIVERSE

Creativa Security Consulting AB is a structural component of the Creativa Center Universe (CCU). It operates as a formally registered and licensed Swedish security company, subordinate to Creativa Center AB and aligned with CCU's overarching governance doctrine. Its placement within CCU is deliberate, reflecting a boundary between internal protective functions and commercially regulated security services.

The Company does not operate as an isolated commercial enterprise. It serves as a professional, compliance-anchored extension of CCU's governance model, ensuring legal defensibility and operational integrity across Creativa's domestic and international activities.

1.1 Organisational Placement

The Company is placed under the Creativa Center AB ownership structure as a wholly-owned subsidiary. It maintains operational independence in order to comply with Swedish licensing regulations, but its strategic mandate is defined by Creativa Center's Board. The organisational logic can be summarised as follows:

Entity / Layer	Role	Nature	Legal Status
Creativa Center AB	Ultimate owner and strategic governor	Governance	Holding Company
Creativa Protective Security Unit	Internal, non-commercial protective services	Strategic	Internal Unit (non-licensed)
Creativa Security Consulting AB	Licensed provider of commercial security services	Operational	Licensed Aktiebolag
EUOS, ECHO, SFPSEI & African Missions	Internal clients and operational environments	Operational	Not applicable

This layered structure preserves the lawful separation required by Swedish and EU regulations while enabling strategic coherence.

1.2 Mission Alignment within the CCU Framework

CCU is constructed as a multi-institutional universe spanning security, education, inclusion, governance, social development, and continental programmes. Within this system, Creativa Security Consulting AB plays a unique role as the "security infrastructure provider" for multiple CCU projects.

The Company's mandate aligns with the CCU through four dimensions:

1. **Protection:** Securing EUOS properties, residents, staff, and visitors.
2. **Resilience:** Enabling safe deployment of ECHO modules and technologies.
3. **Continuity:** Ensuring safe executive, staff, and partner mobility across Europe and Africa.
4. **Ethical Conduct:** Ensuring operations reflect CCU's non-extractive, human-centric mission.

1.3 Relationship with EUOS
EUOS (EUSL Our Society) is a central operational client for both safeguarding and protection. The Company ensures:

- Secure property access and monitoring
- Professional youth-compatible guarding
- Incident response
- Night-time safety infrastructure
- Integration with safeguarding officers
- Compliance with Swedish youth protection regulations

The Company therefore becomes a foundational component of the EUOS model.

1.4 Relationship with ECHO Deployments
ECHO modules, due to their technological and financial value, require structured security:

- Site security
- Storage and transit protection
- Convoy route assessment
- Cooperation with local licensed armed escorts abroad
- Port and airport risk mitigation
- On-site asset integrity systems

The Company serves as the operational security coordinator for all ECHO activities.

1.5 Relationship with Africa Operations (SFPSEI and Beyond)
The Company supports international missions through:

- Cross-continental risk analysis
- Travel advisory
- Convoy planning
- Local security partner integration
- Airport and ground movement coordination
- Emergency and evacuation support

It does not carry weapons abroad. Armed functions are delegated to licensed host-country providers.

1.6 Ethical, Legal, and Reputational Boundaries
The Company is expressly prohibited from:

- Military activity
- Paramilitary activity

- Intelligence operations beyond legal corporate security
- Weapons procurement outside lawful commercial practice
- Activities inconsistent with CCU's governance doctrine

This preserves CCU's standing with governments, RECs, DFIs, and institutional partners.

CHAPTER 2 — MANDATE AND PURPOSE

Creativa Security Consulting AB exists to fulfil a dual mandate: first, to secure the operational integrity of the Creativa Center Universe (CCU) across all domestic and international environments; second, to operate as a licensed and professional security provider capable of delivering selected commercial services consistent with Swedish and EU law and aligned with the ethical principles of CCU. This mandate is both operational and institutional, grounded in the recognition that security, safeguarding, and resilience are indispensable prerequisites for Creativa Center's socio-economic, educational, and developmental missions.

The Company's purpose is to ensure that all Creativa initiatives can operate safely and predictably, regardless of jurisdiction, demographic composition, asset type, or operational context. This includes EUOS properties with young residents and trainees; ECHO deployments involving high-value modular infrastructure; African missions where political, logistical, or socio-economic conditions elevate risk; and the movement of Creativa executives engaged in institutional, governmental, and intergovernmental engagements.

The mandate distinguishes clearly between internal protective services and licensed commercial operations. Internal protective services fall outside the commercial domain and are governed by the Creativa Protective Security Unit, which does not charge for its services and does not require commercial licensing. The Company, by contrast, is licensed under Swedish law to engage in commercial security activities and is authorised to provide guarding, patrols, monitoring, access control, incident response, asset protection, and selected risk advisory services.

The purpose of the Company is therefore not solely economic. It is primarily infrastructural: to provide a lawful, professional, and ethical security environment that enables Creativa operations to function effectively. Profit is permitted but subordinated to legality, safeguarding, and the protection of young people, staff, executives, partners, and the communities Creativa serves.

In practice, the mandate encompasses the following areas: the secure operation of EUOS properties; safeguarding-compatible site protection; executive and staff protection consistent with Swedish and EU legal frameworks; security of ECHO module transport, storage, and installation; security coordination with licensed partners in African jurisdictions; and the establishment of a controlled, compliant expansion path into selective commercial markets.

The Company's mandate, positioned within CCU, is therefore defined not by scale but by responsibility. It is an entity created to uphold institutional integrity, reinforce public trust, protect human life, safeguard high-value assets, and ensure the safe execution of CCU's long-term mission across continents.

CHAPTER 3 — MARKET ANALYSIS

The security market in which Creativa Security Consulting AB will operate is bifurcated between the mature, highly regulated environments of Sweden and the wider European Union, and the fragmented,

risk-variable environments across selected African countries. The Company must therefore understand, and strategically position itself within, two fundamentally different market realities.

The Swedish market is dominated by a small number of major actors—Securitas, Avarn Security, and Nokas—each of which operates under the Swedish Act on Private Security Companies (Lagen om bevakningsföretag). This legal environment establishes strict licensing rules, training requirements, ownership suitability tests, and oversight mechanisms. The market is characterised by stability, high labour costs, regulated guard competence, and strong expectations regarding professionalism and liability management. Within this context, the Company is not intended to compete on volume or scale but on specialisation, quality, and alignment with youth environments and complex property models. EUOS, with its unique combination of residential, educational, social, and vocational structures, represents a niche that traditional security companies do not fully address. The Company therefore enters the Swedish market not as a generalist, but as a specialised provider integrated into a complex societal ecosystem.

At the EU level, regulation varies across Member States but remains generally aligned with Swedish standards regarding licensing, liability, and the prohibition of armed private security in most civilian contexts. The Company's commercial activities within the EU will initially remain limited, with expansion driven primarily by EUOS replication and by specific demand for safeguarding-compatible guarding models.

The African operational environment is structurally different. The Company will not operate as a commercial guarding provider in Africa and will not carry weapons. Instead, the African environment is treated as a risk environment rather than a commercial market. The Company's role is to provide route planning, risk assessments, asset protection strategies, partner oversight, logistics coordination, and cooperation frameworks with licensed local security companies or state-provided units. This model reflects international best practices used by UN agencies, EU missions, DFIs, and diplomatic actors who rely on locally licensed armed teams while retaining strategic control of movement, intelligence, and planning.

In the African context, the primary drivers for security demand are: the transport and protection of high-value ECHO equipment; travel and accommodation security for executives and staff; political or civil instability in certain COMESA, EAC, and SADC jurisdictions; and the general risk profile associated with operating visible, internationalised development programmes. The Company's market position in these environments is therefore not competitive but coordinative.

Across both continents, the Company's competitive advantage stems from its integration with CCU and its ability to combine safeguarding, security, organisational governance, and ethical principles into a unified service model. Large security firms rarely engage with youth-focused environments, educational structures, international development programmes, or multi-jurisdictional risk doctrines. The Company, by contrast, is specifically created to operate within these niches as part of an integrated socio-economic and developmental infrastructure.

The Company's market analysis therefore reveals a carefully defined operational space: specialised, legally compliant, safeguarding-compatible security services in Sweden and the EU, and structured cross-continental risk management and partner coordination in Africa. This positioning enables the Company to fulfil its institutional purpose without entering high-volume competition and without compromising the ethical foundations of the Creativa Center Universe.

CHAPTER 4 — LEGAL AND REGULATORY FRAMEWORK

Creativa Security Consulting AB operates within one of the most regulated sectors in Sweden and the European Union. The legal and regulatory framework governing its activities is not merely a compliance requirement but a structural foundation that defines the Company's permissible conduct, organisational design, and future development. The Company's legitimacy and long-term viability depend on strict adherence to the statutory constraints governing private security operations, both domestically and internationally.

Sweden's legal regime is built around the *Lagen om bevakningsföretag* (The Act on Private Security Companies), which imposes licensing requirements on all entities performing guarding, property protection, monitoring, patrols, access control, alarm response, or similar activities. This legislation requires that owners and board members meet suitability standards; that operations be supervised by an approved Security Manager (*verksamhetsansvarig*); and that all guarding personnel hold government-approved training and certification. The Act also places strict limits on the use of force, the handling of sensitive information, and the legal boundaries between private guarding and public policing. Creativa Security Consulting AB is fully subject to all these requirements and will maintain permanent compliance structures accordingly.

At the EU level, security operations are governed by a constellation of directives and regulations relating to labour law, liability, data protection, workplace safety, and cross-border service provision. Of particular relevance is the General Data Protection Regulation (GDPR), which governs all surveillance systems, monitoring technologies, and incident reporting tools. Any use of cameras, access logs, communications systems, or body-worn technology must therefore meet the GDPR's strict standards of necessity, proportionality, and data minimisation. Within EUOS environments that include young people, the regulatory threshold is further elevated by child protection obligations and heightened data sensitivity norms.

The Company must also comply with Swedish employment legislation, including the Work Environment Act, which mandates safe working conditions for guards, supervisors, and security personnel. These obligations apply equally to night shifts, high-stress interventions, and safeguarding-related incidents on EUOS properties. Additional sectoral requirements stem from the Swedish Criminal Code provisions governing self-defence, excess of force, and unlawful detention. These legal distinctions must be operationalised through training and internal protocols to ensure that all interventions remain lawful, proportionate, and defensible.

International operations introduce a fundamentally separate legal landscape. The Company is prohibited from carrying weapons abroad unless personnel are licensed under host-country law, which is neither planned nor appropriate. In many African jurisdictions, only local security firms or public-sector entities such as police or military units may legally carry firearms or conduct armed escort operations. Accordingly, the Company's international protective posture relies on partnership models, where strategic control, intelligence, and movement planning remain internal, while armed components are delivered by licensed local providers.

The Company is expressly prohibited from engaging in activities that would be classified under host-country law as military, paramilitary, mercenary, or intelligence functions. This prohibition aligns with Swedish legislation, international conventions, and the ethical framework of the Creativa Center Universe. The Company will therefore not procure weapons, engage in armed operations, or perform any duty reserved for state authorities.

This regulatory environment creates a clear operational boundary: all commercial guarding, monitoring, and response activities performed in Sweden or the EU must adhere to licensing requirements; all safeguarding work must integrate with youth protection laws; all data must be handled under GDPR; and all international protective activities must be executed in partnership with legally authorised local actors. The Company's governance, training, and operational frameworks are therefore designed to ensure that every action taken under its mandate is compliant, lawful, ethical, and aligned with the institutional character of CCU.

CHAPTER 5 — ORGANISATIONAL STRUCTURE AND GOVERNANCE

The organisational structure of Creativa Security Consulting AB is designed to balance operational capability with legal compliance, ethical responsibility, and the governance philosophy of the Creativa Center Universe. Because private security is a regulated domain and a high-liability sector, the Company's governance model must embody transparency, accountability, and clear lines of authority. These structural features are not administrative preferences; they are fundamental prerequisites for licensing, oversight, and long-term institutional trust.

The Company is governed by a Board of Directors appointed by Creativa Center AB. Board members must meet Swedish suitability requirements and must not have conflicts of interest or associations that would jeopardise licensing approval. The Board is responsible for strategic direction, legal adherence, financial oversight, and alignment with CCU's ethical framework. It does not interfere in day-to-day operations, which remain the responsibility of management.

Operational leadership is vested in a Chief Executive Officer supported by a management team with expertise in security operations, legal compliance, safeguarding, and international coordination. Central to the governance structure is the Security Manager (*verksamhetsansvarig*), whose appointment is subject to approval by Swedish authorities. This role carries legal accountability for ensuring that all operations, personnel, and methods comply with Swedish private security legislation. The Security Manager oversees all licensed activities, supervises training compliance, and ensures that all operational procedures adhere to statutory requirements.

An internal Compliance Officer ensures adherence to GDPR, workplace safety regulations, safeguarding obligations, reporting duties, and internal ethical standards. This role acts as a bridge between the Company and Creativa Center's central governance infrastructure, ensuring consistency across CCU. The Compliance Officer maintains oversight of all data handling, incident documentation, and cross-border risk considerations.

The organisational structure maintains a clear and intentional separation between the Company and the Creativa Protective Security Unit. The internal unit handles executive protection, internal safeguarding, strategic intelligence, and crisis coordination, while the Company delivers commercial, licensed guarding services. This structural separation preserves legal clarity: the internal unit does not require licensing, while the Company operates under a licensing regime. Information sharing between the two entities is permitted only to the extent required by law and institutional necessity.

A Risk and Oversight Committee, appointed by Creativa Center AB, provides an additional governance layer. This Committee reviews incidents, compliance findings, international partner evaluations, safeguarding concerns, and operational performance. Its mandate is to ensure that the Company does not deviate from legal obligations or CCU principles and that risk exposure remains continuously managed.

Employee governance is equally critical. All guards, supervisors, and monitoring personnel must undergo statutory training and must adhere to the Company's behavioural, ethical, and safeguarding standards. Regular audits are mandated to ensure that employees conduct themselves professionally and lawfully, particularly in youth environments and sensitive contexts.

Finally, the governance model assigns special importance to international operations. A dedicated International Coordination Function ensures that activities in Africa or other regions remain compliant with local laws, partnership agreements, and CCU's risk doctrine. This function liaises with local licensed providers, oversees movement planning, reviews convoy arrangements, and ensures that all activity remains within the scope of lawful protective security and never approaches prohibited or quasi-military domains.

Through this structured, layered, and legally anchored governance model, Creativa Security Consulting AB maintains the institutional integrity required to operate within both Swedish law and the broader Creativa Center Universe. The governance principles reinforce the Company's commitment to legality, ethical conduct, safeguarding of young people, and protection of assets and personnel across multiple jurisdictions.

CHAPTER 6 — SERVICE PORTFOLIO

The service portfolio is designed to provide a lawful, ethically governed, and competence-based suite of security services that directly enable Creativa Center Universe operations while permitting a carefully controlled commercial offering. The portfolio is structured to respect licensing constraints, safeguarding obligations, and the Company's prohibition on military or quasi-military activity. Services are offered first to Creativa entities as internal clients and thereafter, selectively, to external parties where such engagements reinforce the Company's mandate and do not introduce disproportionate risk or reputational exposure.

The Company's principal services in Sweden and the European Union comprise property protection, access control, patrol and response, monitoring and observability, event security aligned with safeguarding, executive movement coordination, and safeguarding-compatible supervision in youth environments. Property protection includes fixed-post guarding, reception security, visitor vetting, and out-of-hours presence to deter intrusion and manage incidents. Access control integrates credential management, guest workflows, and lock-down procedures aligned with data protection law. Patrol and response services are deployed in accordance with licensing conditions, with clear incident categorisation and escalation rules. Monitoring and observability encompass alarm receiving, CCTV oversight, and response coordination, delivered under strict GDPR and child-protection thresholds. Event security for EUOS and related premises emphasises de-escalation, crowd safety, fire safety coordination, and integration with safeguarding officers. Executive movement coordination in the EU remains unarmed and is strictly limited to risk assessment, routing, timing, liaison with local police where appropriate, and the provision of armoured transport where lawfully and operationally justified.

The service set for African operations is defined not as commercial offering but as protective coordination in support of Creativa missions. The Company provides risk assessments, route planning and convoy doctrine, airport and ground movement coordination, vetted-partner management, and site security design for ECHO installations. Armed functions, where necessary and lawful, are executed exclusively by licensed local providers or state entities. The Company retains the strategic layer—intelligence synthesis, itinerary control, convoy discipline, communications integrity, safe-haven

identification, and emergency extraction triggers—thereby ensuring continuity with the Creativa Protective Security Unit while remaining firmly within host-country legal boundaries.

Asset protection for ECHO modules is a distinct service category. It includes secure storage specifications, custody chains, tamper detection, GPS-based movement visibility, and port and airport handover protocols. During transport, the Company prescribes convoy composition, halting rules, and communications discipline, and ensures that local armed escorts, if any, are contracted, briefed, and supervised within the limits of applicable law. On site, ECHO facilities receive layered protection integrating perimeter hardening, illumination, access zoning, alarm integration, and remote monitoring. The Company's role is to design, implement, and audit these controls, not to militarise them.

Safeguarding-compatible supervision at EUOS is a specialised offering tailored to environments with young residents and trainees. It emphasises presence, observation, de-escalation, and early intervention, coordinated with designated safeguarding officers and compliant with reporting thresholds to authorities. This service avoids any conflation of the guard role with therapeutic or pedagogical functions while ensuring that the physical environment remains predictably safe.

To clarify internal versus external applicability, the portfolio can be summarised as follows:

Service Category	**Internal Clients (EUOS, ECHO, CCU)**	**External Clients (Selective)**	**Notes on Legal/Ethical Boundaries**
Property Protection & Access Control	Primary	Selective	Licensed guarding; GDPR-compliant credentialing
Patrol & Alarm Response	Primary	Selective	Within Swedish/EU licensing terms
Monitoring & Observability (CCTV/Alarms)	Primary	Selective	GDPR, data minimisation, child-sensitive processing
Event Security (Safeguarding-aligned)	Primary	Selective	De-escalation emphasis; crowd/fire safety integration
Executive Movement Coordination (EU)	Primary	Limited	Unarmed; liaison with authorities as appropriate
Armoured Transport (EU)	Primary	Limited	Lawful defensive measure; risk-based justification
Africa Protective Coordination (Non-commercial)	Primary	Not offered	Armed components via licensed local/state partners
ECHO Asset Protection (Design & Audit)	Primary	Not offered	Custody and movement visibility; layered site security

Safeguarding-Compatible Supervision (EUOS)	Primary	Not offered	Works alongside safeguarding officers; strict boundaries
Risk Advisory & Partner Due Diligence	Primary	Selective	Non-investigatory, corporate-security scope only

Commercial ambition is intentionally restrained. External engagements are limited to contexts where the Company's standards and doctrine can be upheld without diluting the institutional integrity of the Creativa Center Universe. Any external contract must be subjected to suitability analysis, legal review, and reputational screening, with the default presumption in favour of internal service priorities.

Insurance, indemnities, and service-level undertakings are tailored to each category, with particular care in safeguarding environments and monitoring services where liability and privacy exposures are elevated. Pricing, where applicable, reflects full compliance costs, professional training, audit overhead, and technology lifecycle obligations. The Company does not discount services in a manner that would undermine legal compliance, staff welfare, or safeguarding standards.

CHAPTER 7 — OPERATIONAL MODEL

The operational model translates the Company's mandate into consistent practice across jurisdictions, properties, and mission types. It is designed to be lawful, auditable, and replicable, with a focus on command clarity, personnel competence, technology assurance, and continuous improvement. The model is intentionally conservative, prioritising predictability and legal defensibility over speed or improvisation.

Operations are directed through a central command and control function that maintains real-time situational awareness over guarded sites, patrol assets, alarms, and incidents. This function integrates incident intake, triage, escalation, and documentation, with automated retention controls aligned to data protection policies. Standard operating procedures define incident categories, response thresholds, and handover criteria to public authorities. The command function also coordinates executive movements, armoured transport scheduling where justified, and liaison with local police or emergency services. For international movements, it coordinates itinerary design, safe-haven mapping, communications plans, and vetted-partner deployment, while ensuring that armed components remain the responsibility of licensed local providers or state entities.

Staffing follows a competence-based model. All personnel assigned to licensed guarding roles meet statutory training requirements and receive additional modules in de-escalation, safeguarding awareness, incident documentation, and GDPR-compliant evidence handling. Supervisors are trained in incident command, on-scene decision-making, and coordination with safeguarding officers in EUOS settings. Rostering ensures adequate rest periods, shift overlaps for continuity, and diversity of competencies per shift. Recruitment and vetting include criminal record checks where permitted by law, reference verification, and suitability interviews specifically assessing judgement in youth and mixed-community environments.

Vehicle operations are risk-led. The use of armoured vehicles in Sweden and the EU is governed by a written justification process based on threat assessment, route characteristics, and the profile of the principal or cargo. Drivers receive training in defensive driving, convoy discipline when applicable, radio procedure, and post-incident protocol. Vehicle maintenance and armour integrity checks are

scheduled, logged, and audited. Fuel, communications backups, medical kits, and immobilisation countermeasures are standardised per vehicle type and mission profile.

Technology and data handling are treated as safety-critical systems. Monitoring platforms, access control, radios, and body-worn devices (where used) undergo formal configuration management, change control, and periodic security testing. Data retention is minimised by design; access is role-based; audit trails are immutable; and export of footage or logs is strictly controlled. In safeguarding contexts, additional filters, masking, or redaction may be applied to protect minors and vulnerable persons, with a legal basis documented for every processing activity.

Quality assurance and audit are continuous. The Company maintains an internal audit calendar covering licensing compliance, training currency, incident handling quality, data protection adherence, safeguarding integration, and partner performance in international contexts. Incident reviews include root-cause analysis, lessons learned, policy updates, and feedback to training curricula. Near-miss reporting is encouraged under a just-culture doctrine to surface systemic issues without penalising good-faith disclosures.

Supply-chain and partner governance are embedded in daily operations. Procurement of uniforms, communications equipment, monitoring systems, and vehicles adheres to documented standards on durability, data protection, health and safety, and ethical sourcing. International partners used in Africa or other regions are vetted for licensing status, ownership integrity, human-rights posture, corruption exposure, insurance sufficiency, and operational track record. Contracts with such partners specify lawful scope, reporting duties, incident thresholds, and termination rights in case of breach or misconduct.

The interface with the Creativa Protective Security Unit is formalised. The internal unit retains strategic oversight for executive protection posture, crisis policy, and institutional risk doctrine. The Company executes licensed guarding and commercial operations, provides operational reporting to the internal unit where appropriate, and receives strategic guidance. Information exchange is governed by necessity and legality, ensuring that sensitive data is neither hoarded nor circulated without purpose.

Business continuity and crisis management procedures are rehearsed. Table-top and live exercises cover fire, medical emergencies, missing persons, violent intruder scenarios, data loss, infrastructure outages, and international evacuation. The Company maintains contact trees, alternate communications, redundant monitoring capability, and memoranda of understanding with critical public services and vetted partners.

Labour relations and workforce welfare are recognised as core risk controls. The Company maintains lawful employment practices, fair scheduling, access to psychological support after critical incidents, and continuous professional development. In youth environments, additional supervisory support is provided to front-line staff, acknowledging the heightened emotional and ethical complexity of such contexts.

Financial discipline underpins operations without compromising compliance or welfare. Resource allocation prioritises licensing adherence, training currency, technology reliability, armoured vehicle integrity, and insurance sufficiency. External commercial engagements are subject to operational capacity checks to prevent over-extension and quality erosion. Pricing and cost recovery reflect the true cost of compliant, ethical security operations.

Through this operational model, the Company ensures that its services remain lawful, professional, auditable, and aligned with the ethos and institutional gravity of the Creativa Center Universe. The result is a security capability that protects people and assets, sustains trust with public authorities, and provides a stable platform for EUOS, ECHO, and international mission execution.

CHAPTER 8 — TECHNOLOGY AND INFRASTRUCTURE

The technological and infrastructural foundation of Creativa Security Consulting AB is designed to function as a regulated, resilient, and lawful security architecture capable of supporting complex multi-jurisdictional operations. Technology, within this framework, is not adopted for convenience but is selected and implemented as a direct extension of statutory obligations, ethical commitments, and operational doctrines established under the Creativa Center Universe. Every technological component used by the Company must therefore satisfy three criteria: legal compliance, operational necessity, and governance integrity.

The Company maintains a centralised command and control capability that integrates alarm receiving, surveillance monitoring, incident intake, and operational coordination. This facility operates under strict GDPR conformity, with defined data-retention schedules, role-based access controls, and an immutable audit log of all interactions. Hardware and software configurations follow a controlled change-management protocol to ensure that no system update, integration, or configuration shift compromises security, privacy, or continuity. Internal communications systems rely on encrypted channels with redundancy in case of network failure, ensuring uninterrupted coordination during emergencies or cross-border movements.

Surveillance infrastructure deployed on EUOS sites and other Creativa properties adheres to heightened privacy standards appropriate for environments involving young people. Cameras are placed only where necessary, with signage, masking, geofencing, and restricted access to footage. Audio recording is either disabled or legally justified on a case-by-case basis and subject to review by the Company’s Compliance Officer. Automated alerts for perimeter breaches, restricted area access, and night-time imaging are calibrated to reduce false positives while ensuring timely intervention during genuine threats.

Access control systems are integrated with identity verification processes that respect the principle of minimal data collection. Card-based, token-based, or biometric authentication solutions may be used depending on the risk level of specific facilities. In youth environments, biometric systems are subject to stricter privacy regimes and require documented legal basis and parental or guardian consent where required. All access logs are reviewed periodically to detect anomalies, ensure compliance with data-retention limits, and identify behavioural patterns that may signal safeguarding concerns.

Technology supporting armoured transport and executive movement coordination includes GPS telemetry, panic mechanisms, secure radio communication, and mobile failover channels. Vehicles used for high-risk or high-value transport are equipped with run-flat tyres, protected fuel systems, intrusion-resistant panels, and tracking units with geofenced alerts. These systems interface with the Company's command function, enabling real-time visibility during movements and providing escalation triggers if deviations occur.

Infrastructure supporting ECHO deployments requires a tailored security design. ECHO modules frequently include embedded systems—water, energy, monitoring, communications—that must be shielded from tampering, theft, sabotage, or espionage. The Company’s infrastructure responsibilities include site-hardening designs, alarm integration, motion sensors, tamper-evident seals, secure gates,

lighting arrays, and remote monitoring stations. Ports and airports handling inbound ECHO equipment are subject to pre-deployment audits to ensure custody integrity from offloading to final destination. Routine assessments verify whether local conditions require hardened storage, local guard presence, or partnered armed escort.

Data integrity is reinforced through multi-tier storage architecture, where operational data, safeguarding data, and international risk intelligence are segregated. Backups are encrypted and stored in separate jurisdictions where required by law or operational prudence. Any cross-border transfer of personal data complies with GDPR's transfer regime, and personal data related to minors in EUOS environments receives the highest level of internal restriction.

The infrastructure extends beyond hardware and digital systems to include physical facilities such as guard stations, secure briefing rooms, controlled storage spaces, armour-integrity inspection zones for vehicles, and readiness areas for international coordination. These facilities reflect safety, accessibility, and compliance requirements and are audited for structural integrity, fire safety, and emergency egress.

Through this integrated technological and infrastructural framework, the Company ensures lawful surveillance, secure operations, resilience against disruptions, and the protection of sensitive environments. Technology serves not as an accelerator of intrusive capacity but as an instrument for safe, lawful, and ethical security governance consistent with the Creativa Center Universe.

CHAPTER 9 — TRAINING AND WORKFORCE DEVELOPMENT

The competence and integrity of personnel constitute the primary risk control mechanism for Creativa Security Consulting AB. In a regulated and high-liability sector, the quality of training directly determines the lawfulness, safety, and ethical legitimacy of operations. Accordingly, the Company maintains a comprehensive training and workforce development doctrine that spans recruitment, statutory training, internal standards, safeguarding requirements, cultural competency, and continuous professional development. This doctrine aligns with CCU's broader commitment to human capital development, both within Sweden and across international operations.

All personnel engaged in licensed guarding functions must complete mandatory Swedish security training modules recognised by the national authorities. This statutory foundation is supplemented by Company-specific curricula emphasising de-escalation, lawful intervention, report writing, evidence handling, and behavioural awareness. Given the Company's unique role within CCU, additional training components address safeguarding sensitivity, youth-environment dynamics, and psychological early-warning indicators. Personnel assigned to EUOS environments receive tailored instruction to ensure that their presence complements, and does not replace, the duties of safeguarding officers and pedagogical staff.

Supervisors and team leaders undergo enhanced training in incident command, risk assessment, operational decision-making, and cooperation with emergency services. They are also trained to manage complex environments such as EUOS properties, where security operations must remain anchored in proportionality, respect for residents, and sensitivity to diverse social contexts. Supervisors on international assignments receive further instruction in cross-cultural communication, mission planning, evacuation triggers, and local-partner coordination.

Training for armoured vehicle operations and movement coordination includes defensive driving, communications discipline, convoy behaviour, situational scanning, and post-incident documentation.

Personnel assigned to support executive movements must demonstrate competence in discreet operations, risk-based routing, and lawful interaction with public authorities. They are expressly trained not to exceed the legal limits of private security, including the prohibition of impersonating law enforcement, carrying weapons without lawful authority, or engaging in activities reserved for state actors.

International mission training is delivered through scenario-based modules reflecting African operating environments. This training includes understanding local legal frameworks, corruption-avoidance principles, political neutrality, safety protocols for high-risk zones, and identification of local armed partner capabilities. All personnel involved in international coordination must pass a suitability assessment evaluating judgement, composure under pressure, ethical grounding, and capacity to follow strict protocols.

An internal Training and Standards Division maintains the curriculum, tracks certifications, renewals, incident-related retraining needs, and emerging legal requirements. This Division develops modules jointly with the Creativa Protective Security Unit to ensure consistency between strategic doctrine and operational execution. Training integrates lessons learned from incidents, near misses, audits, safeguarding reviews, and risk analyses.

The Company also contributes to the broader CCU workforce ecosystem by establishing vocational training pathways linked to EUOS and WOFL. These pathways offer opportunities for youth and community members to pursue careers in security, supervision, crisis management, monitoring operations, and protective coordination. By aligning training with CCU's social and educational institutions, the Company transforms security employment from a transactional labour model into a developmental component of the Creativa ecosystem.

Continuous professional development is mandatory. Personnel receive periodic refresher training on legal updates, safeguarding policies, new technologies, and revised operational protocols. Supervisors and managers engage in leadership development programmes emphasising ethical governance, intercultural competency, and institutional accountability. Psychological support and stress-management resources are provided following critical incidents, recognising the emotional and cognitive demands of the profession.

The training and workforce development doctrine therefore ensures that personnel not only satisfy statutory requirements but embody the ethical and institutional standards of the Creativa Center Universe. By investing in human competence, the Company safeguards legality, protects the public, reinforces trust, and ensures that every operational action reflects the principles upon which CCU is built.

CHAPTER 10 — FINANCIAL MODEL

The financial model for Creativa Security Consulting AB is structured to ensure long-term stability, regulatory compliance, operational sufficiency, and alignment with the Creativa Center Universe's ethical and institutional framework. Because the Company operates in a regulated sector where underfunding correlates directly with legal exposure, service degradation, and safeguarding failures, the financial model prioritises resilience over profit maximisation. The Company is therefore capitalised, budgeted, and managed in a manner consistent with risk governance rather than commercial opportunism.

The financial architecture rests on a tripartite structure comprising internal funding streams, external revenue from selective commercial engagements, and controlled capital expenditure for critical infrastructure and armoured transport. Internal funding derives from service-level agreements executed with Creativa Center AB, EUOS, ECHO operations, and other CCU entities. These internal agreements are cost-reflective rather than profit-driven, ensuring that safeguards, regulatory requirements, training, protective technology, and compliance systems are adequately financed. Because safeguarding environments and youth-focused properties impose higher operational standards, internal service fees incorporate the full cost of enhanced training, supervision density, and data-protection compliance.

External revenue is permitted but limited. Commercial engagements with third parties are restricted to contexts where the Company's standards can be upheld without compromising legal integrity or organisational capacity. Pricing for external services reflects actual cost structures, including statutory training, insurance, compliance audits, monitoring infrastructure, equipment depreciation, and supervisory oversight. The Company does not engage in price-driven competition with large-volume security providers; instead, it offers specialised services for clients requiring safeguarding alignment, advanced monitoring integrity, or high-ethics corporate security.

Capital expenditure focuses on technology infrastructure, command and control systems, secure communications, surveillance systems, hardened facilities, and armoured vehicles for domestic executive movement. These acquisitions follow a scheduled lifecycle to ensure reliability and compliance with emerging regulatory standards. Armoured vehicles, in particular, require periodic inspection of ballistic integrity, mechanical resilience, and telematics functionality. Funding for these assets may derive from direct investment by Creativa Center AB, long-term leasing arrangements, or structured financing consistent with Swedish corporate law. No capital expenditure relates to weapons procurement, as such activity is prohibited.

Operating expenses include salaries, training costs, supervisory functions, licensing fees, insurance, maintenance of infrastructure, and partner contracts abroad. The Company maintains liability insurance appropriate for licensed guarding operations, property protection, and safeguarding-compatible supervision. International activities require additional insurance coverage, including kidnap and ransom (K&R) insurance for executives, professional indemnity coverage for risk-assessment activities, and political risk coverage for operations in fragile environments.

A key component of the financial model is the principle of *compliance-first costing*. Security services are priced to ensure that every statutory and internal obligation can be met reliably. Attempts to reduce cost by lowering training intensity, reducing supervisory layers, or delaying infrastructure upgrades are expressly prohibited, as such decisions would increase exposure in both legal and ethical dimensions.

Financial reporting adheres to Swedish accounting standards and incorporates an internal audit cycle aligned with CCU governance requirements. Reports include risk-adjusted provisions, scenario-based stress tests, and long-term budgeting that anticipates growth in EUOS properties, ECHO deployments, and international movement requirements. The Company operates with full transparency toward Creativa Center AB's governance bodies, ensuring that financial discipline reinforces rather than endangers institutional objectives.

Through this financial model, the Company is positioned as a stable, ethically governed, and risk-aware entity capable of supporting CCU operations across jurisdictions while maintaining a sustainable and compliant commercial security presence.

CHAPTER 11 — RISK MANAGEMENT AND LIABILITY

Risk management is a defining pillar of Creativa Security Consulting AB, as the Company operates in a sector where failures can result in legal sanctions, physical harm, reputational damage, and loss of public trust. The risk management doctrine aligns with CCU's governance philosophy, international legal standards, and the Company's mandate to operate both domestically and across complex international environments. The doctrine is intentionally conservative, prioritising harm prevention, statutory compliance, and institutional integrity over operational aggressiveness or commercial expediency.

The Company adopts a layered risk management framework that encompasses strategic, operational, legal, technological, safeguarding, and international dimensions. Strategic risks relate to organisational mandate, licensing exposure, board suitability, and alignment with Creativa Center's governance. Operational risks include failures in guarding duties, insufficient training, improper incident handling, errors during executive movement coordination, and failures in safeguarding-compatible supervision. Legal risks include breaches of the Act on Private Security Companies, GDPR violations, unlawful detention, improper use of force, and cross-border violations of host-country law in Africa or other regions. Safeguarding risks relate to the protection of minors, vulnerable individuals, and youth residents within EUOS environments, where thresholds for reporting, intervention, and escalation are legally and ethically heightened.

Liability management is embedded into all operational decisions. Every security activity—whether patrolling a property, monitoring a site, coordinating an executive movement, or advising on international risk—creates a potential liability vector. For this reason, the Company differentiates between actions that personnel are authorised to take and actions reserved for public authorities. Guards are trained to recognise the boundary between lawful private intervention and unlawful impersonation of police powers. De-escalation is prioritised, and physical intervention is limited to statutory self-defence principles. Any failure to respect these boundaries could result in criminal liability for the individual and regulatory sanctions for the Company.

In safeguarding environments, liability extends to omissions as well as actions. Personnel must report concerns, indicators of abuse, or safety risks to designated safeguarding leads. Silence or inaction can constitute a breach of duty. Accordingly, the Company's safeguarding doctrine emphasises vigilance, accurate documentation, timely escalation, and strict respect for confidentiality and privacy norms.

International operations introduce additional layers of risk. Operating in African jurisdictions exposes personnel to political instability, corruption, infrastructure deficits, local licensing complexity, and cultural variance in law enforcement practices. The Company's doctrine prohibits staff from engaging in any activity that could be construed as military or paramilitary. Risk assessments guide all international movements, defining safe routes, travel windows, hotel suitability, and the necessity of local armed escorts. Liability is mitigated through clear contracts with vetted local security providers, insurance protections, and strict communication protocols. In the event of an incident abroad, the Company follows the crisis escalation pathways defined by the Creativa Protective Security Unit and local authorities.

Technological risks are addressed through cyber-security controls, GDPR compliance, access restrictions, and encrypted communications. Liability for data breaches, unauthorised surveillance, or improper handling of recorded footage is mitigated through training, oversight, and internal audit

protocols. Any technology capable of recording or tracking individuals is subject to legal review before deployment.

A formal incident reporting and review system ensures that every event—whether minor or serious—is documented, analysed, and used to update training and operational guidance. Near-miss reporting is encouraged under a just-culture doctrine that prioritises learning over blame, provided personnel acted in good faith and within the scope of lawful instruction. Regular risk assessments are conducted for EUOS sites, ECHO deployments, and international corridors, capturing dynamic changes in threat levels, community tensions, infrastructure vulnerabilities, and geopolitical factors.

Insurance plays a final, critical role in liability management. The Company maintains comprehensive liability coverage, employer liability insurance, professional indemnity insurance, cyber liability protection, and appropriate international risk policies. All policies are reviewed annually to ensure that coverage remains aligned with operational realities.

Through this integrated approach, Creativa Security Consulting AB maintains a disciplined, ethical, and legally compliant risk and liability posture. This doctrine is essential to protecting individuals, preserving public trust, ensuring regulatory conformity, and supporting the long-term mission of the Creativa Center Universe across Europe and Africa.

CHAPTER 12 — IMPLEMENTATION ROADMAP

The implementation of Creativa Security Consulting AB proceeds in sequenced stages to ensure licensing conformity, operational readiness, safeguarding alignment, and financial sufficiency before any expansion. The roadmap is consciously conservative, with explicit decision gates and non-negotiable compliance milestones prior to the commencement of commercial services or cross-border support. Each stage is anchored in lawful process, documented controls, and auditable standards consistent with the governance doctrine of the Creativa Center Universe.

The initial foundation phase establishes the legal, fiduciary, and organisational prerequisites for a licensed Swedish security company. Board constitution, suitability checks, appointment of the Security Manager subject to authority approval, registration of insurance policies appropriate to guarding and monitoring services, and adoption of statutory policies for data protection and workplace safety are executed in parallel. During this phase, the Company finalises its operating procedures, internal audit calendar, and the separation instruments governing information exchange with the Creativa Protective Security Unit. A pre-licensing compliance review is conducted to ensure that every statutory requirement is met before formal submission.

The capability build phase focuses on recruitment, statutory guard training, enhanced internal modules for de-escalation and safeguarding, command and control stand-up, communications infrastructure, and lawful surveillance deployment for initial EUOS properties. Data protection impact assessments (DPIAs) are completed for each monitoring solution, particularly where young residents and trainees are present. Armoured transport specifications are finalised and vehicles are procured or leased with maintenance, telemetry, and integrity-inspection protocols embedded in the asset lifecycle.

The initial operations phase begins with internal clients only. Licensed guarding is deployed to selected EUOS sites, monitoring is activated under documented DPIAs, incident reporting flows are exercised, and supervisory oversight is stress-tested. Executive movement coordination within Sweden and the EU is commenced on a limited basis with written risk justifications for armoured use where applicable.

ECHO asset protection doctrines are piloted in storage and pre-deployment contexts, with custody and handover protocols validated.

Audit and consolidation follow, with an internal audit of licensing compliance, incident handling, safeguarding integration, DPIA adherence, and insurance sufficiency. Lessons learned are incorporated into revised procedures and training curricula. Only after a satisfactory audit does the Company consider a limited external service offering in Sweden or the EU, and then only where client environments and contractual terms are compatible with safeguarding and compliance duties.

International readiness is developed in parallel on a planning basis. The Company does not offer commercial guarding abroad. Instead, it prepares country readiness dossiers for priority African jurisdictions, including legal landscape reviews, vetted-partner shortlists, airport and port risk notes, convoy doctrines adapted to local conditions, and draft memoranda of understanding with licensed local providers or state entities. No international deployment proceeds without written host-country legal validation, contracted local armed components where lawful and necessary, and explicit approval under the Creativa Protective Security Unit's crisis and international movement doctrine.

For transparency, the implementation sequence and gates are summarised below.

Phase	Timeframe	Objectives	Key Deliverables	Gate / Criteria to Proceed
Foundation	Months 0–3	Legal constitution, licensing preparation, governance installation	Board seated; Security Manager designated; policies adopted; insurance bound; SLA templates with CCU	Independent pre-licensing compliance review completed; submission ready
Licensing & Capability Build	Months 3–6	Licensing approval; recruitment; statutory and internal training; C2 stand-up; DPIAs	License granted; trained personnel roster; command function live; monitoring configurations documented	Authority license in force; DPIAs signed; insurance confirmed; technology validation passed
Initial Operations (Internal)	Months 6–12	Controlled start at EUOS; monitoring activation; incident handling exercises; executive movement coordination	Guarding live at pilot sites; incident and audit logs; armoured transport SOPs in use	Post-implementation audit with satisfactory findings; safeguarding integration validated
Consolidation & Audit	Months 12–18	Full internal audit; procedure refinements; capacity tuning	Audit report; remedial actions closed; updated training curricula	Board acceptance of audit closure; Compliance Officer attestation

Selective External Services (EU/Sweden)	Months 18–24	Careful market entry for aligned clients	Limited external contracts; pricing reflecting compliance costs	Capacity sufficiency test; reputational and legal screening for each client
International Readiness (Africa)	Parallel, wave-based	Dossier preparation; partner vetting; MoUs; evacuation and emergency protocols	Country dossiers; partner contracts; convoy and movement playbooks	Written legal validation; Protective Security Unit approval; insurance confirmation

Budget approvals, procurement authorisations, and workforce allocations are embedded in each gate. Any gate failure or material audit finding pauses progression until corrective measures are implemented and independently verified. No armed function is ever undertaken by Company personnel; all such functions abroad are contracted to legally authorised local entities with strict oversight.

The roadmap culminates in a steady-state operating cadence with internal EUOS and ECHO demands met reliably, a small and carefully curated external client base within Sweden and the EU, and a pre-approved set of international corridors where the Company can coordinate protective movements through vetted local partners. Continuous improvement is institutionalised through the audit calendar, just-culture incident reviews, and routine engagement with Swedish authorities to ensure that the Company's licensing posture remains unimpeachable.

CLOSING STATEMENT

Creativa Security Consulting AB is established as a lawful, ethical, and professional security institution embedded within the Creativa Center Universe. It exists to protect people, assets, and operations without compromising legality, safeguarding obligations, or public trust. It is structurally separated from the Creativa Protective Security Unit to preserve regulatory clarity while remaining strategically aligned to CCU's governance and mission.

The Company's business plan articulates a security capability that is civilian in character, non-militarised in method, and conservative in risk posture. It provides licensed guarding and monitoring in Sweden and the European Union, safeguarding-compatible supervision for EUOS environments, and protective coordination for international activities through lawfully authorised local partners. Weapons are neither procured nor carried by Company personnel. Armoured transport is employed only where justified, documented, and lawful.

The financial model prioritises resilience, compliance, and workforce competence over volume growth. The operational model privileges predictability, proportionality, and de-escalation. Technology is implemented as a regulatorily compliant instrument for safety and accountability, not as a vector for intrusion. Training pathways are designed to elevate professional standards and to create lawful employment opportunities in concert with EUOS and the wider CCU ecosystem.

Upon adoption by the Board of Creativa Center AB and clearance by the relevant licensing authorities, this document shall constitute the governing business plan and institutional charter for Creativa Security Consulting AB. Annexes will be added to incorporate DPIAs, international country dossiers,

insurance certificates, and audit schedules as they are finalised. All prior drafts or memoranda inconsistent with this text are superseded upon formal adoption.

The Company is thereby mandated to proceed with the staged implementation described herein, maintaining full transparency to Creativa Center governance bodies and to competent public authorities. In doing so, it will provide a lawful, dignified, and reliable security capability worthy of the institutional commitments and societal responsibilities of the Creativa Center Universe.