



● CONFIDENTIAL — AUTHORISED RECIPIENTS ONLY

EXECUTIVE PROTECTION AND TRAVEL SECURITY

Executive Protection Planning — CEO Visit, Basra Energy Sector, Iraq

Jurisdiction: Basra, Iraq

EXECUTIVE SUMMARY

Basra represents a HIGH complexity, HIGH threat jurisdiction for executive protection. The primary operational risks are militia activity in the airport-to-site corridor, information leakage through unvetted local assets, and inadequate emergency response preparation.

TARGET LOCATION	CLIENT TYPE	URGENCY
Basra, Iraq	security consultant	priority, 24 to 72 hours
BUDGET	REFERENCE	ENRICHMENT
€5,000–€25,000	OPS-H89BV8	Not enabled

JURISDICTION ASSESSMENT		
COMPLEXITY	SERVICES	THREAT LEVEL
HIGH	LIMITED	HIGH

SOURCES QUERIED





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

Executive Protection Planning — CEO Visit, Basra Energy Sector, Iraq

COMPLEXITY RATING

HIGH

SERVICES AVAILABILITY

LIMITED

THREAT LEVEL

HIGH

KEY FINDINGS & NEXT STEPS

KEY FINDINGS

- Iran-aligned militia groups, including factions affiliated with the Popular Mobilisation Forces (PMF), maintain a significant presence in southern Iraq and have historically targeted international oil sector personnel and facilities.
- The airport-to-site movement phase is the highest-risk period of the visit.
- Unvetted local fixers or security contractors in Basra carry the risk of information leakage to threat actors.
- Medical evacuation protocols, including the nearest suitable facility in Kuwait or Dubai and the mechanism to activate air evacuation, must be confirmed before departure.

NEXT STEPS

- Commission a threat intelligence package for the Basra visit corridor from Control Risks or an equivalent provider within the next 24 hours.
- Contact the energy company's K&R insurer today to confirm coverage and activate any available response consultant or intelligence support.
- Initiate vendor engagement with at least two Tier 1 international security consultancies within 48 hours to confirm local CP support availability and cost.

MATTER SUMMARY

A European energy company's CEO is scheduled to make a two-day visit to an oilfield facility in the vicinity of Basra, Iraq, flying via Basra International Airport. The UK close protection (CP) provider has a ten-day planning window, a defined budget of €5,000–€25,000, and requires a structured security plan covering the threat picture, airport-to-site movement, ground support requirements, and cost parameters. The principal is a high-profile corporate executive whose presence in southern Iraq, while operationally routine for the energy sector, carries meaningful personal risk exposure requiring professional mitigation.

The primary challenges are the compressed planning timeline, the need to integrate UK-based CP principals with vetted Iraqi ground support assets, and the operational complexity of coordinating movement across a security environment that includes militia activity, kidnap-for-ransom risk, and variable law enforcement reliability. The visit coincides with an environment in which international energy executives have historically been targets of surveillance, opportunistic criminality, and in some periods politically motivated threat. Getting the threat assessment, movement protocols, and local liaison right before departure is the central professional obligation of this engagement.

JURISDICTION PROFILE

Country: Iraq

City: Basra

Complexity Rating: HIGH

Professional Services Availability: LIMITED

Threat Level: HIGH





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

THRESHOLD ASSESSMENT

WHAT MUST HAPPEN IN THE TARGET JURISDICTION:

Physical ground preparation is genuinely required in Basra and cannot be substituted remotely. Specifically:

- Advance route reconnaissance of the airport-to-site corridor must be conducted in person, as road conditions, checkpoint locations, and militia presence points change frequently and cannot be reliably assessed from open-source data alone.
- Local close protection or security liaison personnel must be engaged and physically present throughout the visit to provide armed or unarmed support, cultural translation, and institutional access to local security authorities.
- Liaison with the Basra Operations Command or facility security management at the oilfield must occur on the ground to confirm site access protocols, emergency evacuation routes, and medical support arrangements.
- Safe house or emergency refuge identification and pre-clearance cannot be conducted remotely with adequate reliability.

WHAT CAN BE DONE REMOTELY OR FROM THE CLIENT'S OWN JURISDICTION:

- The full threat and intelligence assessment can be prepared in the UK using commercial threat intelligence feeds, open-source intelligence, and vendor briefings from established risk consultancies with Iraq desks. This is the preferred first step and should be completed before any local engagement is commissioned.
- Communications planning, equipment procurement (encrypted devices, tracking systems, satellite comms), and medical kit preparation can all be handled from the UK.
- Background verification of proposed Iraqi ground support vendors can be partially conducted remotely using Control Risks, G4S, or similar providers' existing vetted partner networks.
- Crisis management protocols, emergency contact trees, and home-country embassy notification can be prepared entirely from the UK.
- Briefing documents for the principal and any travelling party can be drafted and delivered remotely.

WHAT THE CLIENT CAN DO THEMSELVES, TODAY, AT NO COST:

- Register the CEO's travel with the relevant European country's embassy in Baghdad and the consular section monitoring Basra. The UK Foreign, Commonwealth and Development Office (FCDO) Iraq travel advisory is publicly available and should be reviewed immediately.
- Review the oilfield operator's existing site security protocols and standing emergency procedures — the host energy company almost certainly has an HSE or security department with a Basra footprint.
- Contact the energy company's insurer to confirm whether the CEO's travel is covered under the existing policy and whether a kidnap and ransom (K&R) endorsement is active. K&R insurers often provide pre-travel intelligence and response support at no additional cost to the premium holder.
- Begin OSINT review of current Basra security conditions using ACLED, UN OCHA situation reports, and FCDO/US State Department advisories.

PROPORTIONALITY:

The value at stake is not financial recovery but personal safety and organisational liability. A CEO-level executive travelling to an active risk environment in southern Iraq represents a significant duty-of-care obligation. Professional engagement at the mid-to-upper range of the stated budget is proportionate and appropriate. The €5,000–€25,000 budget is realistic for a two-day, professionally managed executive protection operation in this environment, though it sits at the lower end of what Tier 1 providers would charge for full-service support in Iraq.

THRESHOLD CONCLUSION:

This matter genuinely requires both remote preparation in the client's home jurisdiction and physical engagement on the ground in





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

Basra. The two tracks are complementary, not alternatives. Remote threat intelligence and planning work should begin immediately and run in parallel with local vendor engagement. The visit cannot be safely managed with UK CP assets alone operating without local support.

KEY CONSIDERATIONS

1. The Basra security environment is materially different from the rest of Iraq. Iran-aligned militia groups, including factions affiliated with the Popular Mobilisation Forces (PMF), maintain a significant presence in southern Iraq and have historically targeted international oil sector personnel and facilities. This is the primary threat vector and must anchor the threat assessment.
2. The airport-to-site movement phase is the highest-risk period of the visit. Route selection, vehicle configuration, timing, and convoy discipline are critical planning variables. Fixed schedules and predictable routes must be avoided. A counter-surveillance route and a primary and alternate route must be pre-cleared in advance.
3. Local ground support must be vetted before engagement. Unvetted local fixers or security contractors in Basra carry the risk of information leakage to threat actors. Any local partner should be sourced through an established international security consultancy with an existing Iraq network, not through direct cold recruitment.
4. Medical and emergency evacuation planning is non-negotiable. The nearest facility with adequate trauma care for a Western principal is unlikely to be a local Basra hospital. Medical evacuation protocols, including the nearest suitable facility in Kuwait or Dubai and the mechanism to activate air evacuation, must be confirmed before departure.
5. Communications security is an operational requirement. Iraq's signals environment is permissive for interception. The CEO and CP team should travel with encrypted communications capability. Mobile phones should be treated as compromised. The CEO's itinerary, identity, and travel dates should be protected on a strict need-to-know basis within both the energy company and the CP team.

INTELLIGENCE NOTICE

This report was generated WITHOUT live intelligence enrichment. All firm names, contact details, regulatory references, and fee estimates are AI-generated and have not been verified against live data sources. Independent verification of all specific recommendations is required before operational use. To generate a source-backed report with live database screening across 14 sources, enable Live Intelligence Enrichment and provide the subject name.

STRATEGIC APPROACHES

APPROACH 1 — STANDARD

Method: UK CP provider leads the full operation using remote threat intelligence from open-source and subscription tools (ACLED, OSAC, FCDO, Control Risks Country Risk daily), supplemented by the host energy company's existing site security infrastructure. No independent local vendor is engaged. The CP team travels with full equipment and relies on the oilfield operator's security team for site-level support and a pre-arranged vehicle and driver from a known international provider already operating at the site.

Timeline: 7–10 days planning; 2-day visit execution.

Estimated Cost: €3,500–€6,000 (threat intelligence subscriptions or one-off reports: €500–€1,500; vehicle and local driver from site-affiliated provider: €800–€1,500; CP team travel costs and daily rate differential: €2,000–€3,000).

Recommended for: Engagements where the oilfield operator has a robust, established on-site security infrastructure and can genuinely backstop local support requirements. Not recommended if the site security team is a thin-staffed HSE function rather than a trained protective security operation.

APPROACH 2 — ACCELERATED (RECOMMENDED)



CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

Method: UK CP provider engages a mid-tier international risk consultancy with an established Iraq/Basra footprint to provide a dedicated threat intelligence package and vetted local CP support team. Recommended consultancies include those with active Basra operations rather than regional offices only. Local team provides: advance route reconnaissance, armoured vehicle with vetted drivers, liaison with Basra Operations Command, site security coordination, and emergency protocol integration. UK CP lead retains command authority throughout.

Timeline: 5–7 days to stand up local support; 2-day visit execution.

Estimated Cost: €12,000–€20,000 total. Breakdown: threat intelligence and advance planning package: €2,000–€3,500; local CP team (2 personnel, 2 days plus preparation days): €4,000–€7,000 at Middle East multiplier (0.4–0.6x of baseline adjusted for Iraq conflict uplift); armoured vehicle with driver, 4 days including advance: €2,500–€4,000; comms equipment and logistics: €1,000–€2,000; contingency reserve: €1,500–€3,500.

Recommended for: This engagement as described. The ten-day window is sufficient to execute this approach with a competent local vendor. This approach manages the principal threat vectors — route exposure, information leakage, and emergency response — without requiring a full Tier 1 retainer.

APPROACH 3 — EXPEDITED

Method: Full-service engagement with a Tier 1 risk and security consultancy (Control Risks, G4S Government Solutions, Olive Group/Constellis, or equivalent) as the primary operational lead. Tier 1 provider assumes full in-country coordination including: detailed advance work, dedicated intelligence cell monitoring during the visit, multiple-vehicle convoy with counter-surveillance, liaison with both the energy company's security director and local authorities, and a 24/7 operations room function. UK CP provider integrates as the principal's personal detail under Tier 1 command structure.

Timeline: Can be stood up in 3–5 days by a Tier 1 provider with existing Iraq presence.

Estimated Cost: €22,000–€28,000. Note: This approaches the upper boundary of the stated budget. A full Tier 1 Iraq executive protection engagement typically starts at €25,000 for the scope described. Some cost compression is achievable where the UK CP provider absorbs personal detail costs within their own fee structure.

Recommended for: Situations where the threat assessment identifies elevated specific risk to this principal or this visit, where the energy company's risk committee requires a fully documented professional security management structure, or where prior incidents at the facility or against comparable executives have occurred.

LEGAL & REGULATORY FRAMEWORK

Iraq does not have a comprehensive private security regulation framework equivalent to Western jurisdictions, though the Iraqi government has issued various decrees and ministry orders governing the operations of private security companies (PSCs) since 2010. International PSCs operating in Iraq are required to hold a licence issued by the Iraqi Ministry of Interior. This licensing requirement applies to organisations conducting security operations in-country and is a material compliance consideration when selecting a local partner — unlicensed operations create legal exposure for the energy company, the CP provider, and the principal personally. Any local vendor engaged should be asked to produce evidence of current Ministry of Interior PSC licensing before contract execution.

The energy company's UK parent will be subject to UK duty-of-care obligations under the Health and Safety at Work Act 1974 and the Corporate Manslaughter and Corporate Homicide Act 2007. These create a documented obligation to conduct a suitable and sufficient risk assessment for the CEO's travel, implement proportionate controls, and retain evidence of both. The security plan produced from this engagement should be structured to satisfy that evidentiary requirement, not merely to guide operational decisions. A written threat assessment, documented mitigation measures, and a signed-off travel authorisation from the energy company's board or risk committee are minimum requirements.

Insurance is a parallel legal consideration. Most corporate K&R policies require pre-notification of high-risk travel and impose conditions on security arrangements. The energy company's broker and K&R insurer should be contacted before departure confirmation. Failure to



CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

notify can void coverage. Some K&R policies provide access to response consultants and intelligence services as a policy benefit – these should be activated immediately if available, as they represent substantial value at zero additional cost.

PROFESSIONAL SERVICE PROVIDERS REQUIRED

TYPE: International Security Consultancy with Iraq Presence

ROLE: Threat intelligence package, local CP team provision, armoured vehicle logistics, route reconnaissance, and emergency protocol coordination.

QUALIFICATIONS TO LOOK FOR: Active licence to operate in Iraq; verifiable Basra operational history; ASIS International accreditation or equivalent; named account manager with Iraq experience; references from energy sector clients.

TYPICAL COST RANGE: €8,000–€20,000 for this scope in this jurisdiction (Middle East multiplier with conflict uplift applied).

HOW TO VERIFY CREDENTIALS: Request Iraqi Ministry of Interior PSC licence number and verify via the company's Iraqi legal representative; check ASIS International member directory; request client references from comparable energy sector engagements.

CONFIDENCE LEVEL: HIGH

TYPE: Local Iraq Liaison / Fixer (Basra-based)

ROLE: Cultural and linguistic facilitation, checkpoint liaison, local authority contact management, real-time local intelligence during visit.

QUALIFICATIONS TO LOOK FOR: Must be sourced through the international security consultancy above — not independently. Direct cold engagement of local fixers in Basra without vetting through an established international partner is a security risk, not a cost saving.

TYPICAL COST RANGE: €500–€1,200 for 4–5 days including preparation, sourced through a vetted channel.

HOW TO VERIFY CREDENTIALS: Vetting to be conducted by the international security consultancy as part of their service delivery.

CONFIDENCE LEVEL: HIGH

TYPE: Medical Evacuation Provider

ROLE: Standby medical evacuation capability from Basra to Kuwait City, Dubai, or Amman in the event of medical emergency or trauma.

QUALIFICATIONS TO LOOK FOR: EURAMI or CAMTS accreditation; confirmed availability of fixed-wing air ambulance from Basra or regional hub; named medical director; Iraq operational history.

TYPICAL COST RANGE: €1,500–€3,000 for a standby retainer for 2 days; actual evacuation costs vary significantly and should be covered by the energy company's travel insurance or K&R policy.

HOW TO VERIFY CREDENTIALS: Verify accreditation via EURAMI member directory at eurami.org; confirm Iraq operational licences with provider.

CONFIDENCE LEVEL: HIGH

TYPE: Encrypted Communications Supplier

ROLE: Provision of encrypted handsets or satellite communications devices for the CP team and principal during the visit.

QUALIFICATIONS TO LOOK FOR: Experience supplying to CP operations in Middle East environments; devices should be clean, registered outside Iraq, and not linked to the energy company's corporate network.

TYPICAL COST RANGE: €400–€800 for device rental and configuration for a 5-day window.

HOW TO VERIFY CREDENTIALS: Procurement through the security consultancy's existing supply chain is preferred; alternatively





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

through established providers such as TELE2 Satellite or equivalent specialist suppliers.

CONFIDENCE LEVEL: MEDIUM

RECOMMENDED LOCAL FIRMS & CONTACTS

SERVICE TYPE: International Security Consultancy — Iraq Operations

FIRM NAME: Control Risks Group

WEBSITE: controlrisks.com

WHY SUITABLE: Control Risks maintains an active Iraq operational presence including Basra and has a dedicated energy sector practice. They provide threat intelligence, executive protection, and ground logistics in southern Iraq and are routinely engaged by international oil companies operating in the Basra governorate.

HOW TO MAKE CONTACT: Via the enquiry form on the firm's website, specifying Iraq executive protection and referencing the Basra energy sector and timeline.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: International Security Consultancy — Iraq Operations

FIRM NAME: G4S Government Solutions / Allied Universal Government Services

WEBSITE: g4s.com

WHY SUITABLE: G4S has an established Middle East and Iraq footprint with energy sector clients and can provide armoured vehicle logistics and local CP support in Basra governorate.

HOW TO MAKE CONTACT: Via the corporate enquiry route on the firm's website, specifying Iraq close protection and executive movement.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Specialist Risk Advisory — Iraq Energy Sector

FIRM NAME: Olive Group (now part of Constellis)

WEBSITE: constellis.com

WHY SUITABLE: Constellis/Olive Group has deep Iraq energy sector experience and has provided executive protection for international oil company personnel in southern Iraq including Basra-adjacent oilfield environments.

HOW TO MAKE CONTACT: Via the enquiry form on the firm's website.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Medical Evacuation Standby

FIRM NAME: International SOS

WEBSITE: internationalsos.com

WHY SUITABLE: International SOS operates a network covering Iraq and Gulf states, provides standby medical evacuation retainers, and has experience supporting energy sector personnel in Basra governorate. They also provide pre-travel medical risk briefings.

HOW TO MAKE CONTACT: Via the corporate enquiry form on the firm's website or through the energy company's existing corporate account if one is held.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

CONFIDENCE LEVEL: HIGH

RISK & COMPLIANCE CONSIDERATIONS

The principal risk to the UK CP provider is operating in Iraq without an adequate legal framework governing their presence and weapons carriage, if armed. UK-based CP operatives do not have automatic authority to carry firearms in Iraq. Any armed element of the operation must be provided by a locally licensed PSC. The UK CP team, if unarmed, is operating lawfully as a protective advisory and physical presence resource, but must ensure their role is clearly documented to avoid misclassification under Iraqi law governing foreign security personnel. The energy company should obtain written legal advice from an Iraq-experienced law firm before the visit confirming the legal basis of the security arrangement.

From a corporate compliance perspective, the energy company must ensure that all payments to Iraqi vendors, local fixers, and security contractors comply with the UK Bribery Act 2010. Facilitation payments to Iraqi officials — for example to smooth checkpoint passage or accelerate access approvals — are not permitted under the Act regardless of local custom. The security plan must explicitly address how the team will manage checkpoint encounters without making prohibited payments. This is not merely a legal formality: it is a live operational issue in the Basra environment where informal payments at checkpoints are common.

Data security is a compliance risk that is frequently underweighted in executive protection planning. The CEO's itinerary, personal details, flight information, and accommodation data constitute personal data under UK GDPR if held by the UK CP provider. Sharing this data with Iraqi vendors, even vetted ones, requires a legal basis and appropriate safeguards. The CP provider should minimise information shared with local assets to operational need only, and should not transmit detailed itinerary data over unencrypted channels. Post-visit, all itinerary data held by local vendors should be confirmed as deleted.

LOCAL CONTEXT

Basra is Iraq's second-largest city and the centre of the country's oil industry, producing the substantial majority of Iraq's export revenue. The international oil sector presence — including BP, Shell historically, and numerous service companies — means that executive visits by foreign energy company personnel are operationally routine and local infrastructure for supporting them exists. However, routine does not mean low-risk. The presence of Iran-aligned militia factions within and around Basra, periodic rocket and mortar attacks on energy infrastructure, and a history of targeting of foreign oil company employees mean that complacency is the primary operational risk. The security environment has historically been more stable than central and northern Iraq but is sensitive to regional political fluctuations, particularly in relation to Iran-Iraq relations and intra-militia tensions.

The oilfield facilities near Basra — including those associated with the West Qurna, Rumaila, and Zubair fields — typically maintain their own perimeter security and have established emergency protocols for international staff. The quality of this security varies by operator and contract period. The UK CP provider should request and review the facility's current site security plan and emergency evacuation procedures before departure, and should confirm whether the facility has a dedicated security manager or whether security is managed through HSE. The airport-to-site road corridor passes through areas of variable security condition and should not be treated as routine transit.

SECURE WORKING PRACTICES

All planning communications for this visit should be conducted over encrypted channels (Signal or equivalent) and access to the itinerary should be restricted to named individuals within the energy company and the CP team. The CEO's name, title, travel dates, and route should not appear in any unencrypted email. The local security vendor should be briefed on a need-to-know basis with itinerary confirmation given as late as operationally viable. Devices taken into Iraq should be clean travel devices not linked to corporate networks, and the CEO should be briefed to treat all hotel Wi-Fi and public networks as hostile. Post-visit, all devices should be subject to a security review before reconnection to any corporate system.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

RECOMMENDED APPROACH

The recommended approach for this engagement is Approach 2 — Accelerated. Given the ten-day window and the threat environment in Basra, the UK CP provider should immediately initiate parallel workstreams: the remote intelligence and planning track should begin today, and the local vendor engagement track should begin within 48 hours.

The sequenced steps within this approach are:

1. Commission a threat intelligence package from Control Risks or equivalent for southern Iraq/Basra, specifying the visit dates, route corridor, and facility type.
2. Contact the energy company's K&R insurer and confirm coverage, policy conditions, and whether response consultant support is available.
3. Engage a vetted local security vendor through one of the Tier 1 consultancies identified above — do not attempt direct cold recruitment of local assets.
4. Request the oilfield facility's current site security plan and confirm the identity and contact details of the on-site security manager.
5. Confirm medical evacuation standby with International SOS or equivalent.
6. Conduct communications and equipment preparation in the UK: encrypted devices, tracking, satellite comms if required, medical kit appropriate to the environment.

The operation should proceed with a minimum of two UK CP operatives travelling with the principal, supported by a local two-person team. The local team assumes route and checkpoint liaison; the UK team maintains principal proximity throughout. Command authority remains with the UK CP lead.

TIMELINE & MILESTONES

- (1) Days 1–2: Commission threat intelligence package; contact K&R insurer; initiate local vendor engagement through Tier 1 consultancy; brief energy company security director.
- (2) Days 2–4: Receive threat intelligence briefing; confirm local vendor selection and contract; begin communications equipment procurement; request facility site security plan.
- (3) Days 4–6: Local vendor conducts advance route reconnaissance; confirm primary and alternate routes; identify medical facilities and emergency refuge points; confirm medevac standby.
- (4) Days 6–8: Full security plan documented and reviewed by UK CP lead and energy company; CEO principal briefing conducted; communications protocols confirmed.
- (5) Days 8–9: UK CP team travels to Basra; link-up with local support team; conduct ground familiarisation; confirm all emergency contacts and protocols.
- (6) Days 9–10 (Visit): CEO arrives; airport reception protocol executed; movement to site under security plan; site visit conducted; return movement to airport; CEO departs; debrief.
- (7) Day 10–11: Post-visit security debrief; incident report if applicable; device security review; K&R insurer notification of visit completion.

Confidence rating: High for timeline achievability given the ten-day window. The primary dependency risk is vendor response time from Tier 1 consultancies — engagement should begin within 24 hours of this briefing.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

CONTINGENCY CONSIDERATIONS

The primary contingency requiring pre-planning is a deterioration in the security environment during the visit window that requires early termination and emergency extraction. This scenario should be pre-built into the security plan with defined trigger criteria — not left to in-the-moment judgment. Triggers should include: a militia attack within 20km of the route corridor or facility; a credible specific threat against the energy company or its personnel; a closure of Basra International Airport; or a directive from the energy company's crisis management team. The local security vendor should have confirmed relationships with a fixed-wing or rotary extraction capability that can be activated within a defined response time. This should be tested as part of the advance work.

If the stated budget proves insufficient to engage a Tier 1 or strong mid-tier consultancy for the full scope, the energy company's existing oilfield operator relationships should be leveraged before cost-cutting the security package. Operators active in Basra — including those managing Rumaila and West Qurna — have established security departments and vetted local contractor rosters that may be accessible to the visiting CEO's company through the commercial relationship. This route is not a substitute for independent security planning but can provide verified local assets at lower cost and with higher trust levels than cold vendor engagement. For independent vetted vendor sourcing, the ASIS International member directory at [asisonline.org](https://www.asisonline.org) and the Security Institute member search at [security-institute.com](https://www.security-institute.com) are appropriate starting points.

PROFESSIONAL FEES ESTIMATE

The recommended Approach 2 engagement budget is €12,000–€20,000 for the full operation. Threat intelligence package from a specialist provider: €2,000–€3,500. Local CP support team (two operatives, preparation days plus two-day visit): €4,000–€7,000 at applicable Middle East/conflict uplift rates. Armoured vehicle with vetted driver, four to five operational days: €2,500–€4,000. Medical evacuation standby retainer: €1,500–€2,500. Communications equipment rental and configuration: €400–€800. Contingency reserve: €1,500–€2,200. These figures apply the Middle East jurisdiction multiplier (0.4–0.6x baseline) with a conflict zone uplift for Iraq, and reflect realistic market rates for the Basra security services market as sourced through international operators. The full Approach 2 total sits within the stated budget ceiling of €25,000.

The UK CP provider's own fees are not included in the above — these are assumed to be within the provider's existing commercial arrangement with the energy company. If the UK CP team's daily rates and expenses are to be absorbed within the €25,000 ceiling, the local support package should be held at the lower end of the range and the threat intelligence element scoped to a single report rather than an ongoing monitoring subscription. The K&R insurer's response consultant service, if available under the policy, should be activated as it may absorb part of the intelligence cost at no incremental expense.

EXECUTIVE SUMMARY & RECOMMENDED NEXT STEPS

Basra represents a HIGH complexity, HIGH threat jurisdiction for executive protection. The primary operational risks are militia activity in the airport-to-site corridor, information leakage through unvetted local assets, and inadequate emergency response preparation. The recommended approach is Approach 2 — Accelerated, engaging a vetted local security support team through an established international consultancy with an active Iraq presence, supported by a purpose-commissioned threat intelligence package and confirmed medical evacuation standby. This approach is proportionate to the risk, achievable within the ten-day window, and falls within the stated budget. Sanctions screening has not been performed by this system and must be conducted independently by the energy company's compliance function before any vendor payments are executed.

1. Commission a threat intelligence package for the Basra visit corridor from Control Risks or an equivalent provider within the next 24 hours.
2. Contact the energy company's K&R insurer today to confirm coverage and activate any available response consultant or intelligence support.
3. Initiate vendor engagement with at least two Tier 1 international security consultancies within 48 hours to confirm local CP support availability and cost.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

4. Request the oilfield facility's current site security plan and the name of the on-site security manager from the energy company's operations team.

5. Prepare and issue a formal written risk assessment and travel authorisation document to satisfy the energy company's UK duty-of-care obligations before the CEO's departure.

If the recommended approach is followed within the stated timeline, the CEO's two-day Basra visit will be supported by a professionally integrated security operation that mitigates the principal threat vectors, satisfies the energy company's duty-of-care requirements, and positions the UK CP provider to manage both routine movement and emergency contingencies effectively.

--- END OF BRIEFING ---





BLACKBOX

OPERATIONAL INTELLIGENCE

OPS-H89BV8

11 Oct 2026 · 18:33 UTC



CONFIDENTIAL — AUTHORISED RECIPIENTS ONLY



BLACKBOX

OPS-H89BV8 · END OF REPORT

NEAR-ZERO RETENTION

This report was generated on demand and delivered once. It is not written to any database and is discarded from server memory 15 minutes after generation. Save this PDF in a secure location with access restricted to authorised recipients.

Generated: 11 Oct 2026 · 18:33 UTC

Reference: OPS-H89BV8

Classification: Confidential

[blackbox.fyi](#)