Enhanced vetting practices to meet the need of Australia’s Critical Infrastructure

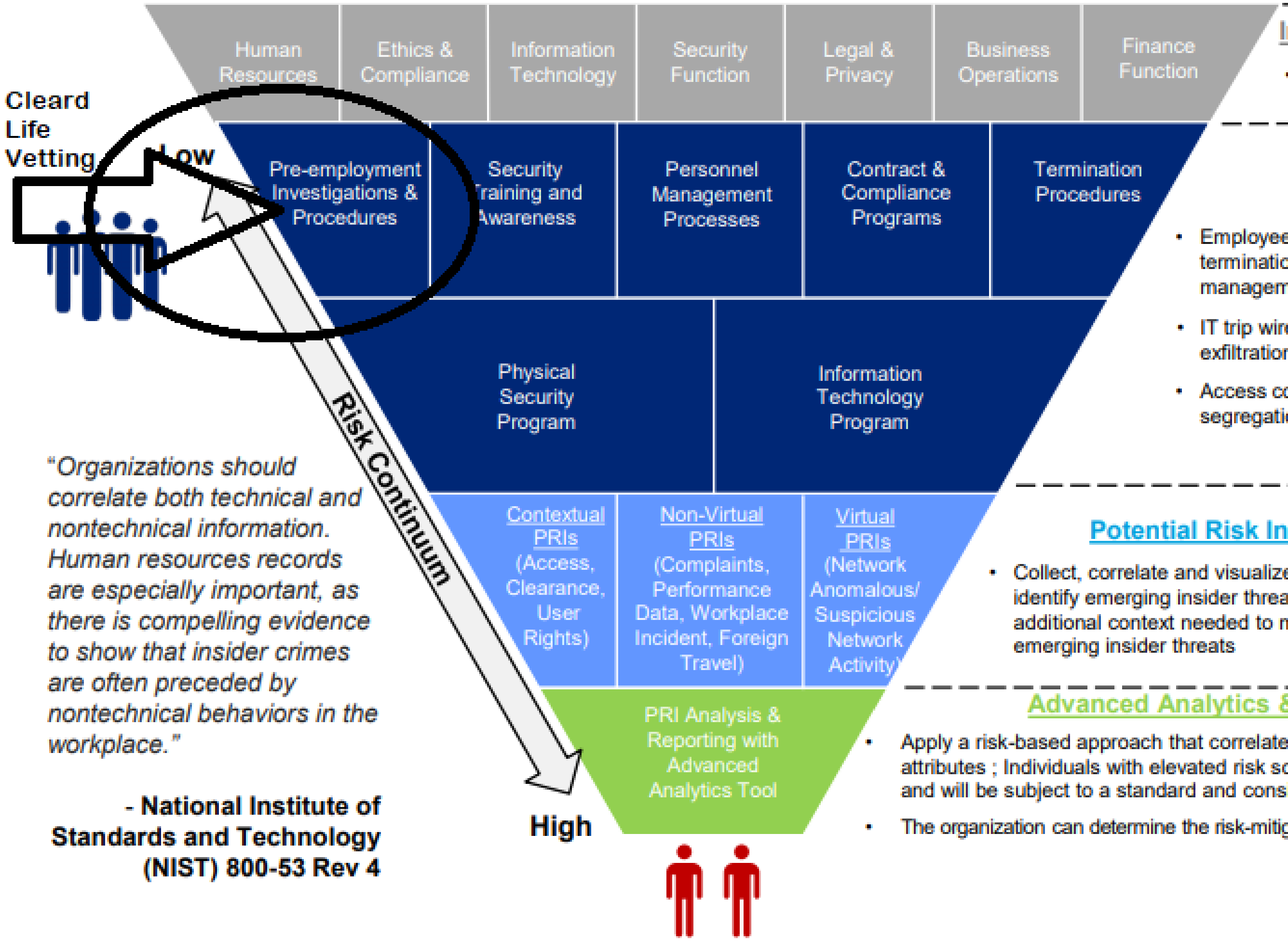
Personnel Security

ISM P10 "Only **trusted** and **vetted** personnel are granted access to systems, applications and data repositories.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

What are the foundational components of an insider threat program?

This framework captures the organizational components necessary for a holistic and risk-based insider threat program. This structure incorporates the prevent, detect, and respond framework, capitalizes on existing capabilities, and promotes stakeholder coordination.



Human Resources
Ethics & Compliance
Information Technology
Security Function
Legal & Privacy
Business Operations
Finance Function
Cleard Life Vetting
Low
Pre-employment Investigations & Procedures
Security Training and Awareness
Personnel Management Processes
Contract & Compliance Programs
Termination Procedures
Physical Security Program
Information Technology Program
Risk Continuum
Contextual PRIs (Access, Clearance, User Rights)
Non-Virtual PRIs (Complaints, Performance Data, Workplace Incident, Foreign Travel)
Virtual PRIs (Network Anomalous/ Suspicious Network Activity)
PRI Analysis & Reporting with Advanced Analytics Tool
High

"Organizations should correlate both technical and nontechnical information. Human resources records are especially important, as there is compelling evidence to show that insider crimes are often preceded by nontechnical behaviors in the workplace."

- National Institute of Standards and Technology (NIST) 800-53 Rev 4

Insider Threat Working Group (ITWG)

- Cross functional representatives meet routinely to discuss insider threat mitigation

Program Foundation

- Employee lifecycle procedures including hiring and termination processes, investigation coordination, case management, and security education programs
- IT trip wires including anomaly detection from common exfiltration points (e.g., e-mail, removable media)
- Access control procedures including least privilege and segregation of duties procedures

Potential Risk Indicator (PRI)* Aggregation

- Collect, correlate and visualize PRIs from a variety of sources in order to identify emerging insider threats; this provides the organization with additional context needed to make an informed decision on how to address emerging insider threats

Advanced Analytics & Escalation and Triage

- Apply a risk-based approach that correlates and assigns risk scores to behaviors and attributes ; Individuals with elevated risk scores will be the focus of risk mitigation efforts and will be subject to a standard and consistent escalation and triage process
- The organization can determine the risk-mitigating action (e.g. inquiry, interview, or intervention).

This approach transcends the traditional focus on technology and takes a holistic and risk-based approach inclusive of business processes, policies, technology, and training.

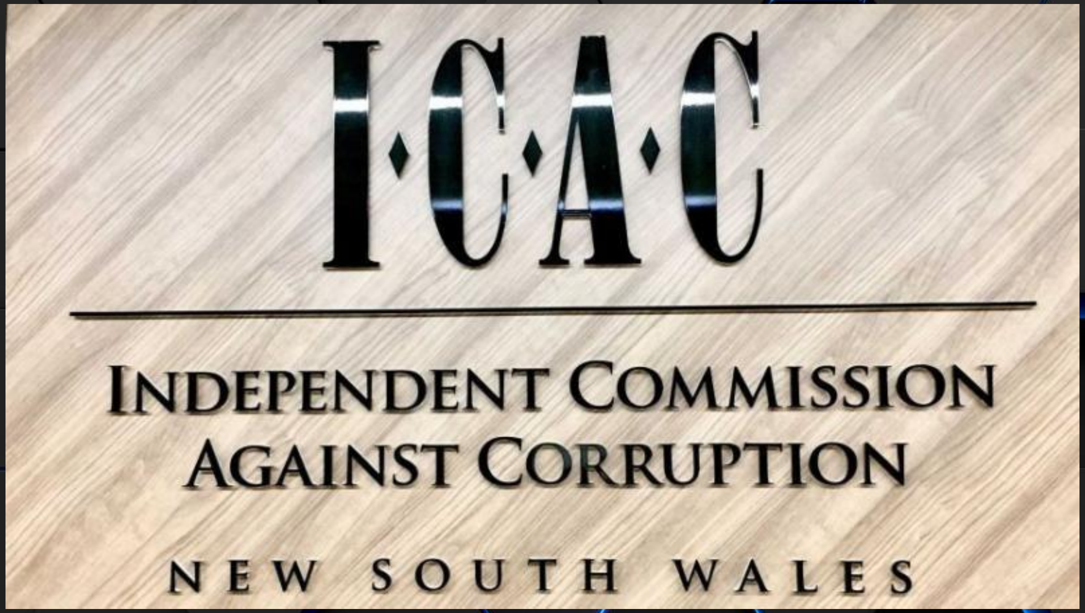
* Potential Risk Indicator (PRI): An action, event, or condition that precedes the insider act and is hypothesized to be associated with the act. The observable precursors (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers, network anomalies) contribute to increased risk. (Source: CERT)

ISM	**Cyber Security Principle: Protect: P10** **"Only trusted and vetted personnel are granted access to systems, applications and data repositories." Security Control 0434 "Personnel undergo appropriate employment screening before being granted access to a system and its resources."**
ISO/IEC 27001	A.7 Human resource security. A.7.1 Objective: To ensure that employees and contractors are **suitable** for the roles for which they are considered. "When an individual is hired for a specific information security role, organisations should make sure the candidate can be trusted to take on the role."
AS 4811	Pre-employment Screening: used as a **basis** for industry or organisational specific screening policies and procedures. The objective is to ensure the **integrity**, **identity** and **credentials** and to provide assurance that they are **worthy** of **trust**.
PSPF	PSPF 12 PERSEC details the pre-employment screening processes and **standardised** vetting practices to be undertaken when employing personnel and contractors.
Critical Industry Sector: eg. DISP	"Each entity must ensure employees and contractors meet an appropriate standard of integrity and honesty."

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

	What EXACTLY happens?
AS 4811 Employment Screening	Identity – **must** sight some form of photo identification. Identity – **must** verify address history. (A driver’s license meets these first two elements.) Integrity – CV **should** be checked. Integrity – Referees **should** be checked. Integrity – Police check **should** be conducted. Credentials – Professional Referee **should** be sought to verify positions and dates of employment from CV. Credentials – verify qualifications and professional memberships
ISO/IEC 27001:2013	A.7.1.1 Implementation guidance a) satisfactory character references b) a verification (for completeness and accuracy) of the applicant's CV c) confirmation of claimed academic and professional qualifications d) independent identity verification (passport or similar document) e) **other** checks as appropriate
Critical Industry Sector: **DISP**	Pre-employment screening is to be in line with AS 4811-2006 and other extra activities might include: • identity checks • eligibility to work in Australia • employment history checks • residential history checks • referee checks • personal employment contracts • non-disclosure agreements • non-compete clauses

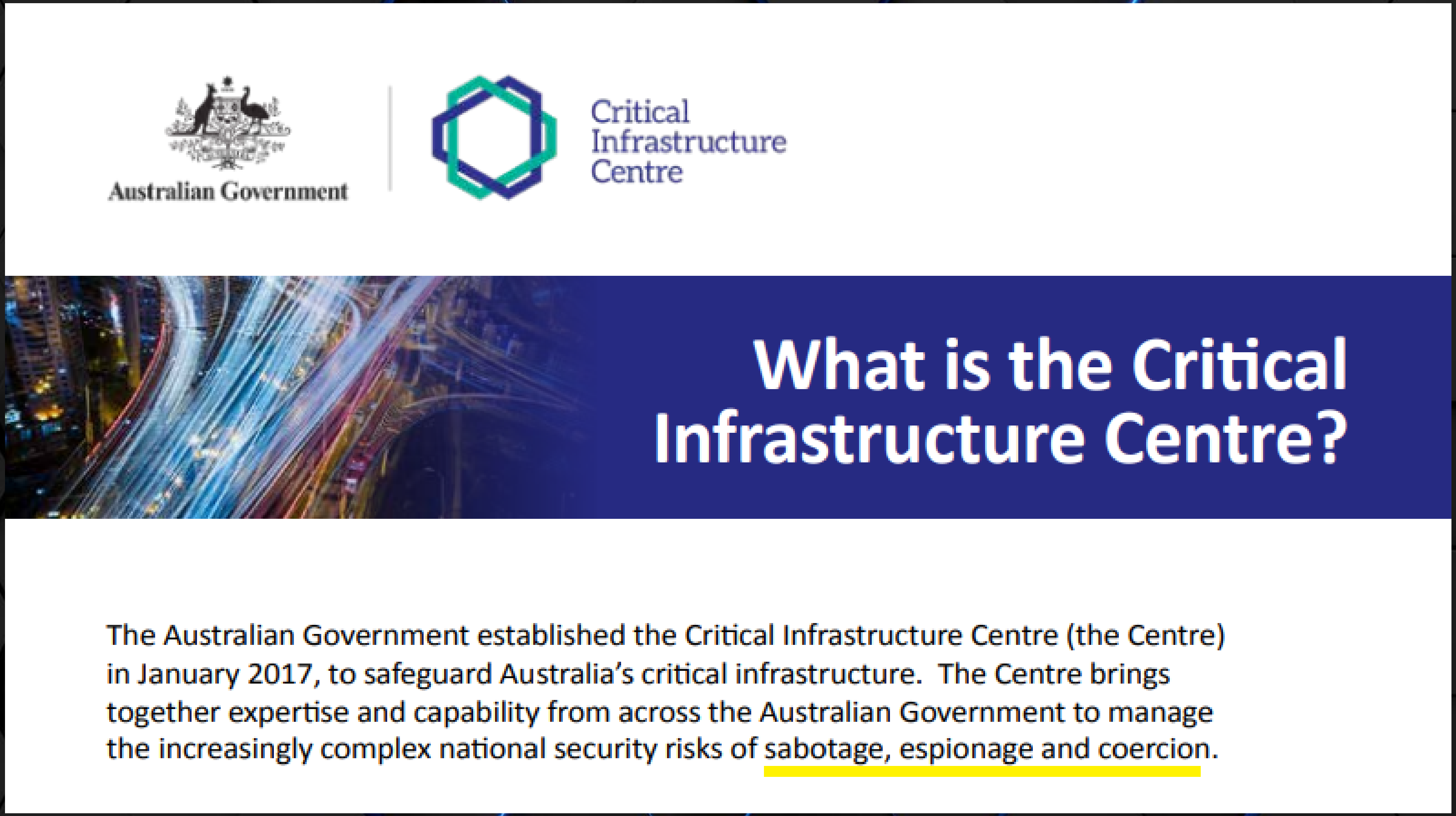
CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE



White paper: Strengthening employment screening practices: "Employers should have a robust process for responding to red flags that arise from employment screening checks."

Employment Screening Handbook: "Employment screening typically consists of checking a candidate’s identity. There are better practices available to inform employment screening such as the Protective Security Policy Framework (PSPF) & the Personnel Security Protocol."

	Protective Security Policy Framework
PSPF 12 details the pre-employment screening processes and standardised vetting practices to be undertaken when employing personnel and contractors	• **Must** assure a personnel and contractors **suitability** and recommends AS4811. • Pre-employment screening is mandatory and recommended that pre-employment checks be applied to provide a level of assurance about the individual's **suitability**. • **Additional** entity-specific [read sector-specific] checks can further mitigate security threats applicable to the entity that are not addressed by 4811 minimum pre-employment screening. • Recommends that suitability screening is done **prior** to employment contract offer!
Minimum	a) Verify a person's **identity** (Document Verification Service?) b) Confirm **eligibility** to work in Australia c) Obtain assurances of a person's **suitability**.
Suitability is defined in the PSPF as HTTMLR:	**honesty** – truthful and frank and does not have a history of unlawful behaviour **trustworthiness** – responsibility, reliability and maturity **tolerance** – an appreciation of the broader perspective even when holding strong personal views, able to remain impartial and flexible **maturity** – capable of honest self-appraisal and able to cope with stress **loyalty** – a commitment to Australia and the democratic processes of the Australian Government. **resilience** – ability to adapt well in the face of adversity, trauma, tragedy, threats or significant sources of stress
PSPF **NATIONAL SECURITY BASELINE CLEARANCE**	• Verification of identity • Confirmation of citizenships (questionnaire) • Referee checks (eg 5 point professional questionnaire) • Digital footprint check • National police check • Financial history check (questionnaire) • Background check - 5 years (questionnaire) • The suitability assessment is to consider their **integrity** in accordance with the Personnel Security Adjudicative Guidelines.

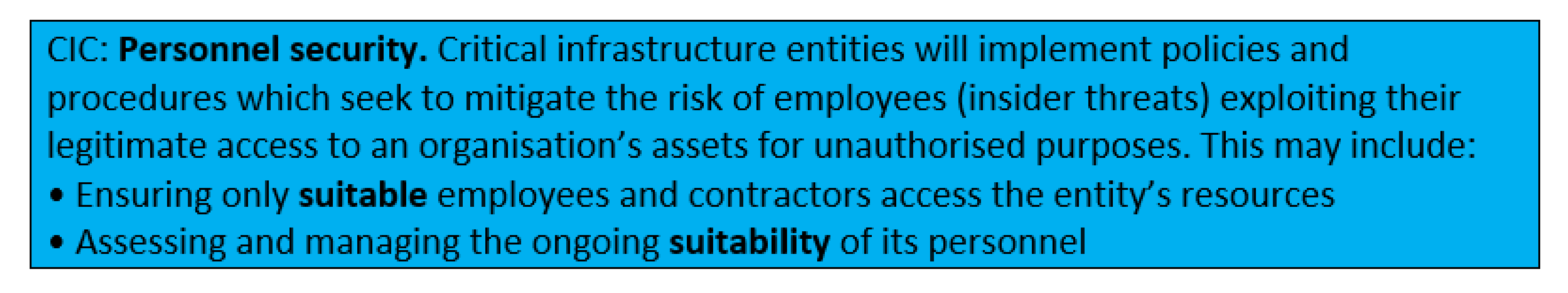


Australian Government

Critical Infrastructure Centre

What is the Critical Infrastructure Centre?

The Australian Government established the Critical Infrastructure Centre (the Centre) in January 2017, to safeguard Australia's critical infrastructure. The Centre brings together expertise and capability from across the Australian Government to manage the increasingly complex national security risks of sabotage, espionage and coercion.



CIC: **Personnel security.** Critical infrastructure entities will implement policies and procedures which seek to mitigate the risk of employees (insider threats) exploiting their legitimate access to an organisation's assets for unauthorised purposes. This may include:

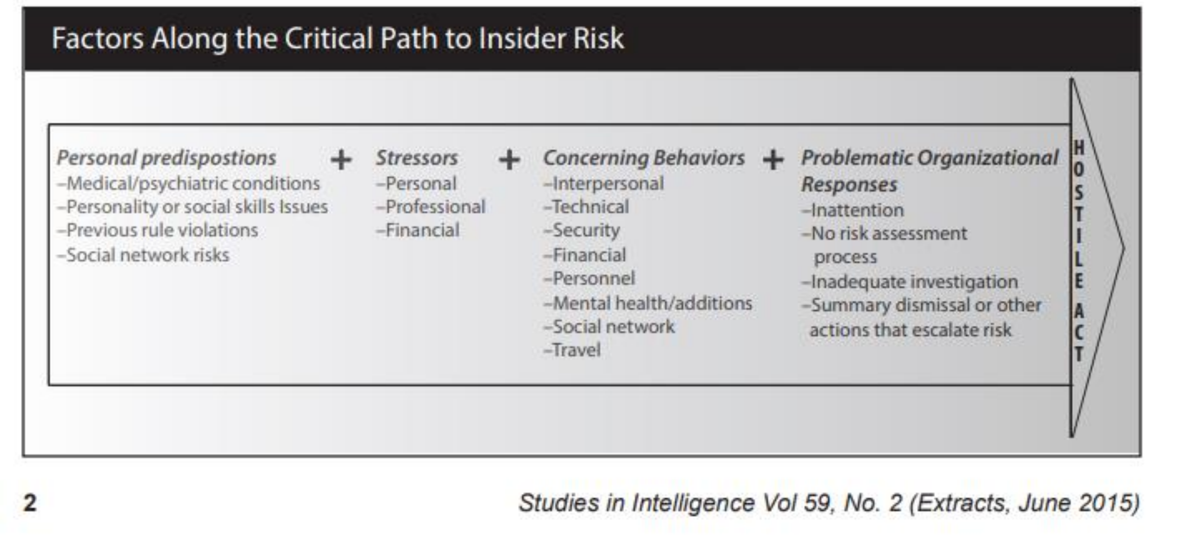
- Ensuring only **suitable** employees and contractors access the entity's resources
- Assessing and managing the ongoing **suitability** of its personnel

Problem: Preemployment screening practices do not usually involve national security risks such as counter-espionage, investigations into coercion risk or sabotage risk assessments.

Something more sophisticated is required … and at scale.

CLEARD LIFE

THE MISSING PIECE IS A CLEARD LIFE



Factors Along the Critical Path to Insider Risk

Personal predispostions + *Stressors* + *Concerning Behaviors* + *Problematic Organizational Responses*

Personal predispostions
- –Medical/psychiatric conditions
- –Personality or social skills Issues
- –Previous rule violations
- –Social network risks

Stressors
- –Personal
- –Professional
- –Financial

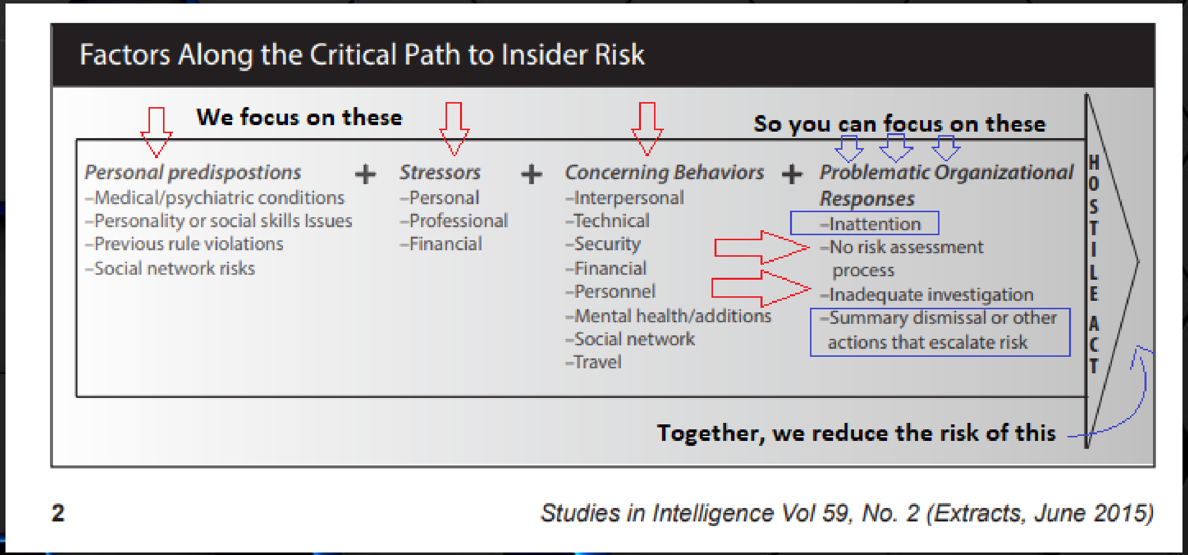
Concerning Behaviors
- –Interpersonal
- –Technical
- –Security
- –Financial
- –Personnel
- –Mental health/additions
- –Social network
- –Travel

Problematic Organizational Responses
- –Inattention
- –No risk assessment process
- –Inadequate investigation
- –Summary dismissal or other actions that escalate risk

HOSTILE ACT

2

Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)



Factors Along the Critical Path to Insider Risk

We focus on these

So you can focus on these

Personal predispostions + *Stressors* + *Concerning Behaviors* + *Problematic Organizational Responses*

Personal predispostions
- –Medical/psychiatric conditions
- –Personality or social skills Issues
- –Previous rule violations
- –Social network risks

Stressors
- –Personal
- –Professional
- –Financial

Concerning Behaviors
- –Interpersonal
- –Technical
- –Security
- –Financial
- –Personnel
- –Mental health/additions
- –Social network
- –Travel

Problematic Organizational Responses
- –Inattention
- –No risk assessment process
- –Inadequate investigation
- –Summary dismissal or other actions that escalate risk

HOSTILE ACT

Together, we reduce the risk of this

2

Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)

Many security personnel vetting programs around the world now use the ‘critical path to insider risk’ protocol which evaluates candidates background for specific personal predispositions, stressors and concerning behaviours.

It predicts or anticipates a trusted insider threat with great efficacy.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

PSPF	Personnel security adjudicative guidelines
Assess the individual against common risk factor areas to support the assessment of a person's suitability.	The seven risk factor areas: - external loyalties, influences and associations - personal relationships and conduct - financial considerations - alcohol and drug use - criminal history and conduct - security violations - emotional and mental health issues.
external loyalties, influences and associations	A security risk may exist when they or their immediate family (including cohabitants and other persons to whom they may be bound by affection, influence or obligation) are not Australian citizens or may be subject to duress.
personal relationships and conduct	Personal conduct, or concealment of information about conduct, that creates a vulnerability to exploitation, manipulation or duress, such as engaging in activities which, if known, may affect the person's personal, professional or community standing. Violation of a written or recorded commitment made by them to the employer as a condition of employment. Association with persons involved in criminal activity.
financial considerations	They are financially overextended and may be at a heightened risk of engaging in illegal acts including espionage to generate funds.
alcohol and drug use	Use of illegal drugs or misuse of prescription drugs can raise questions about trustworthiness and honesty because it may impair judgement and a person's ability or willingness to comply with laws, rules and regulations is questioned. The use of illegal drugs or misuse of prescription drugs may make them vulnerable to coercion or influence.
criminal history and conduct	Criminal activity creates doubt about a person's judgement, reliability, trustworthiness, maturity and honesty. It calls into question a person's ability or willingness to comply with laws, rules and regulations.
security violations	Deliberate or negligent failure to comply with procedures, rules and regulations for protecting sensitive or security classified information, including on ICT systems, raises doubt about a person’s trustworthiness, judgement, reliability or willingness and ability to safeguard such information, and is a serious security concern.
emotional and mental health issues.	Certain emotional, mental and personality conditions can impair judgement, reliability or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

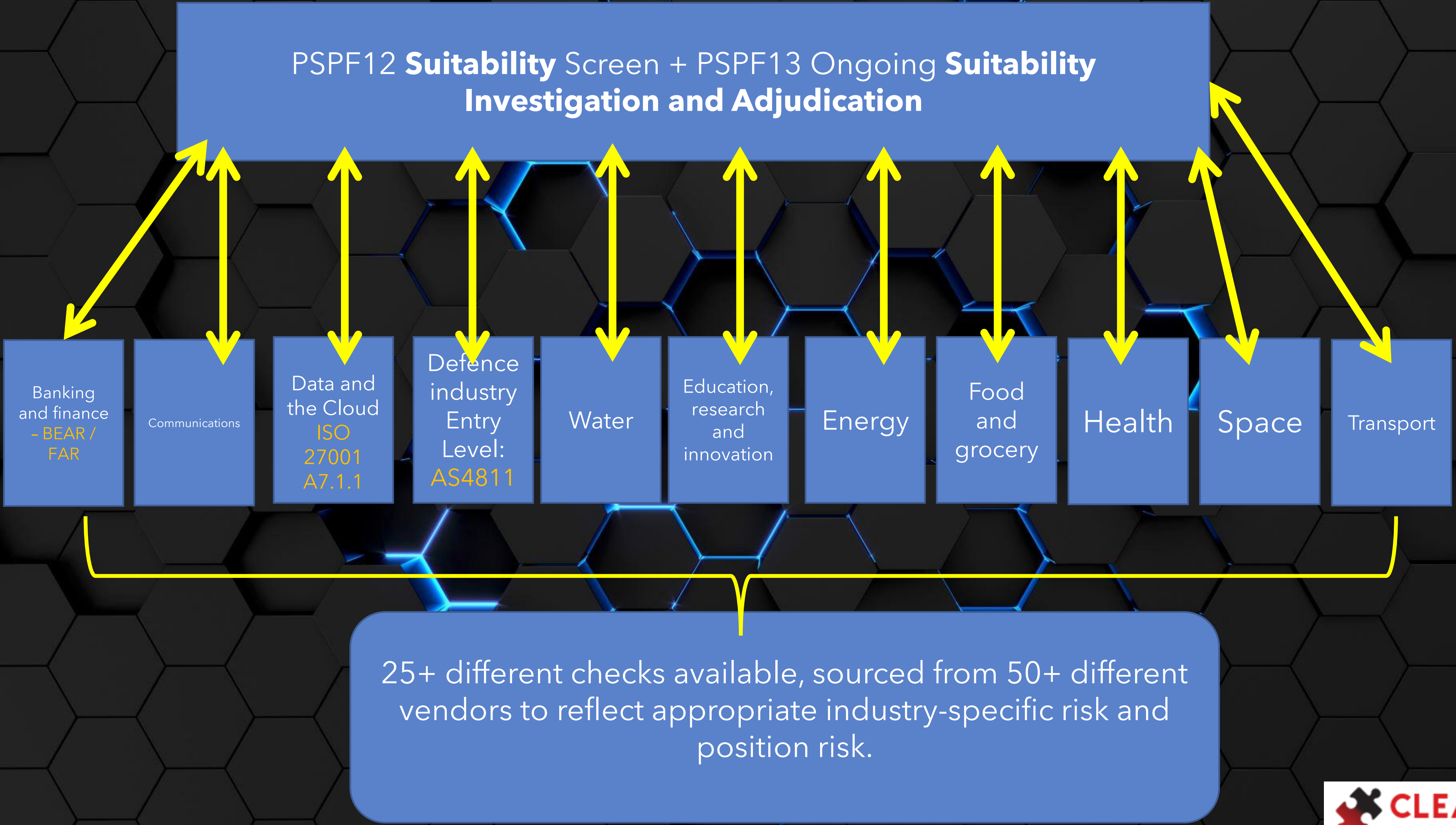
Critical Infrastructure Industry Entities

See the difference between a check and an assessment.

Discussion questions.

- **PERSEC DISCUSSION …**
- **Anticipating your sector's agreed specific requirements and risk based roles, your entity will need to choose up to 25 or more checks from a marketplace of 50+ vendors. (Consider that some hard data 'database' checks are automated, semi-automated and other checks are soft, manual and slow.)**
- **Who is best to administer and coordinate checks: inhouse HR-Security teams, external providers, Application Tracking System providers and/or some hybrid combination?**
- **Who is best to adjudicate red flags that arise from employment screening checks? An in-house team? An outsourced team? Should be have a candidate appeal mechanism? Is there a non-discriminatory, unbiased process to follow?**
- **Consider 1:4 complaints to the Human Rights Commission is due to criminal history discrimination.**
- **Are adverse findings fairly investigated, discussed with the candidate and can the analysis and final decision be audited for compliance, to ensure due process and natural justice?**
- **Should our sector consider a transferable pre-employment suitability clearance to reduce duplication and on-boarding delays?**

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE



PSPF12 **Suitability** Screen + PSPF13 Ongoing **Suitability** **Investigation and Adjudication**

- Banking and finance – BEAR / FAR
- Communications
- Data and the Cloud ISO 27001 A7.1.1
- Defence industry Entry Level: AS4811
- Water
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport

25+ different checks available, sourced from 50+ different vendors to reflect appropriate industry-specific risk and position risk.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

Q. How is suitability determined?

PSPF12 Determining suitability

The determination of whether an individual is suitable to hold a clearance is based on careful consideration of the **whole person** in the context of the following risk factor areas:

a.external loyalties, influences and associations

b.personal relationships and conduct

c.financial considerations

d.alcohol and drug usage

e.criminal history and conduct

f.security attitudes and violations

g.mental health disorders.

These factor areas may have a bearing on one or more of a subject's character traits (HTTMLR).

The Attorney-General's Department recommends vetting agencies use a process of **structured professional judgement** to come to an overall determination based on the available information.

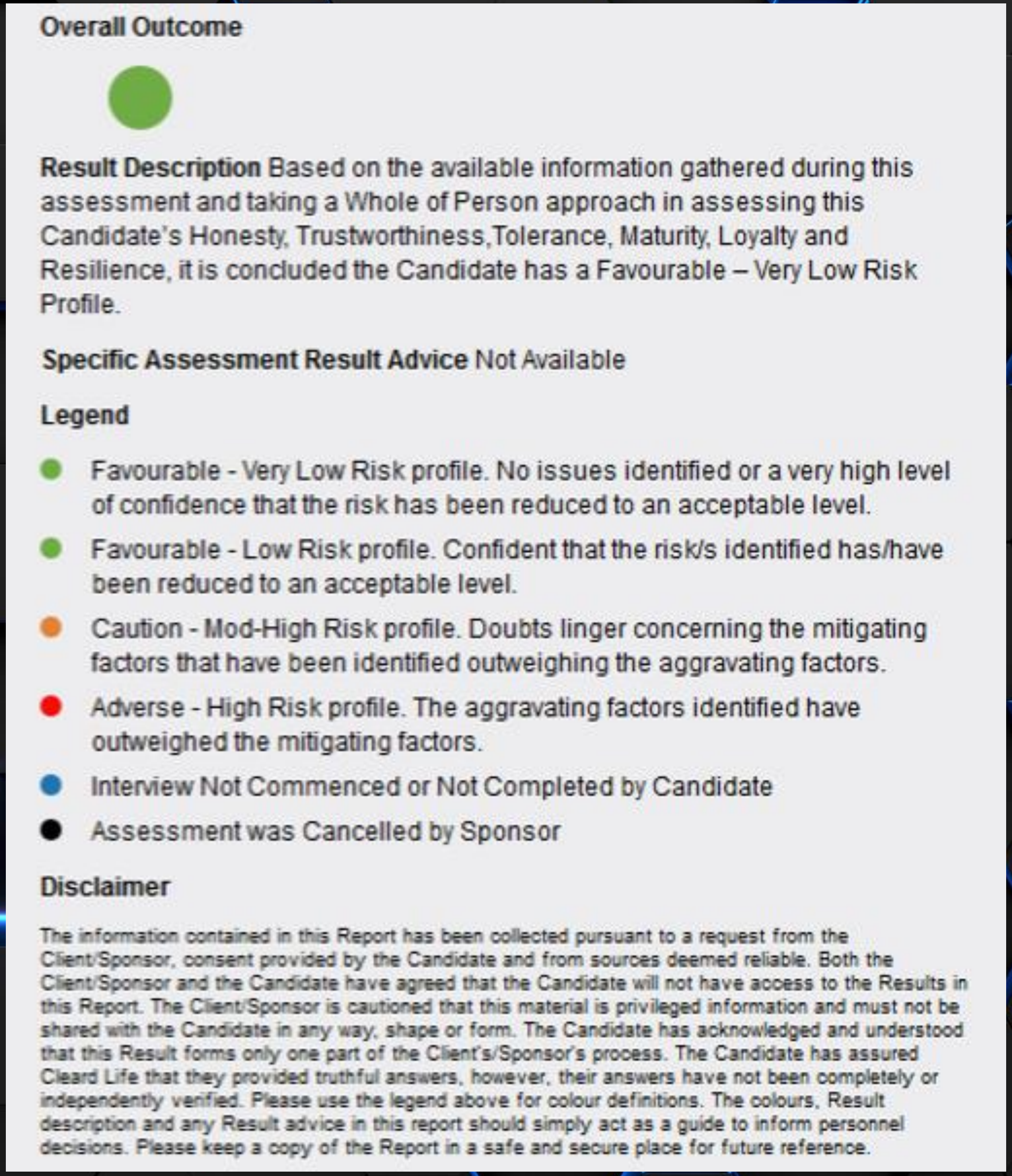
Q. What if some of our workers live overseas, and/or not Australian citizens – how will they be eligible?

That's the difference between a National Security Clearance and a Civilian Suitability Clearance that is able to cater for the complexity of a modern workforce.

The PSPF also delineates between eligible & suitable.

NB: The suitability factor area 'External loyalties, influences and associations' must still be considered: "A security risk may exist when a subject or their immediate family (including cohabitants and other persons to whom they may be bound by affection, influence or obligation) are not Australian citizens or may be subject to duress. These situations could potentially introduce foreign influence that could result in the compromise of information. Contacts with citizens of other countries or financial interests in other countries are relevant to determinations if they make the subject potentially vulnerable to coercion, exploitation or pressure."

Cleard Life Result:



Overall Outcome

🟢

Result Description Based on the available information gathered during this assessment and taking a Whole of Person approach in assessing this Candidate's Honesty, Trustworthiness,Tolerance, Maturity, Loyalty and Resilience, it is concluded the Candidate has a Favourable – Very Low Risk Profile.

Specific Assessment Result Advice Not Available

Legend

- 🟢 Favourable - Very Low Risk profile. No issues identified or a very high level of confidence that the risk has been reduced to an acceptable level.
- 🟢 Favourable - Low Risk profile. Confident that the risk/s identified has/have been reduced to an acceptable level.
- 🟠 Caution - Mod-High Risk profile. Doubts linger concerning the mitigating factors that have been identified outweighing the aggravating factors.
- 🔴 Adverse - High Risk profile. The aggravating factors identified have outweighed the mitigating factors.
- 🔵 Interview Not Commenced or Not Completed by Candidate
- ⚫ Assessment was Cancelled by Sponsor

Disclaimer

The information contained in this Report has been collected pursuant to a request from the Client/Sponsor, consent provided by the Candidate and from sources deemed reliable. Both the Client/Sponsor and the Candidate have agreed that the Candidate will not have access to the Results in this Report. The Client/Sponsor is cautioned that this material is privileged information and must not be shared with the Candidate in any way, shape or form. The Candidate has acknowledged and understood that this Result forms only one part of the Client's/Sponsor's process. The Candidate has assured Cleard Life that they provided truthful answers, however, their answers have not been completely or independently verified. Please use the legend above for colour definitions. The colours, Result description and any Result advice in this report should simply act as a guide to inform personnel decisions. Please keep a copy of the Report in a safe and secure place for future reference.

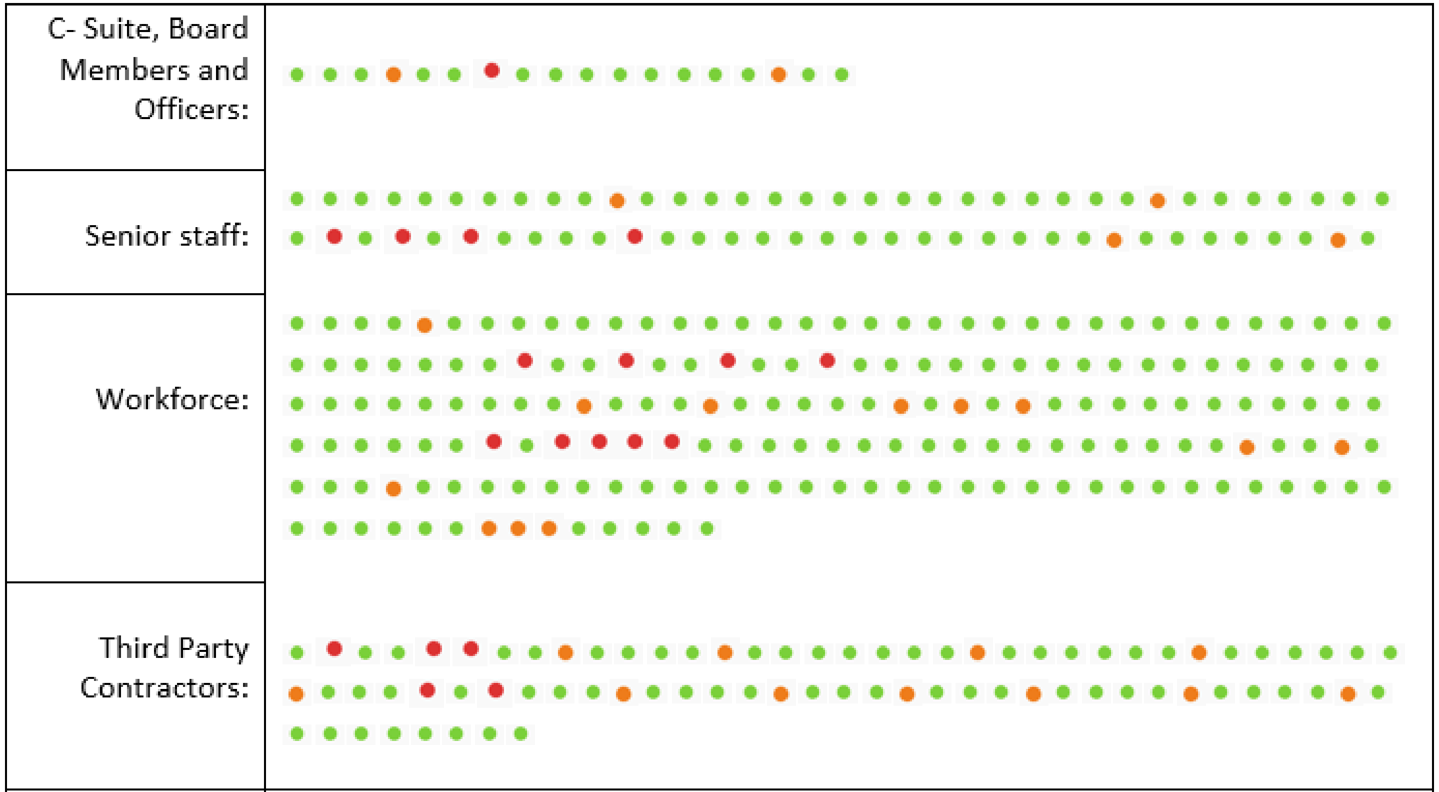
Q. What if we get a red light result or an orange light result as part of pre-employment screen?

1. Use the result to inform your hiring decision
2. Vetting agency may recommend (eg) other measures or a higher level assessment that expands datapoints
3. Information sharing option. 3-way consent with risk mitigation conditions. Vetting agency can set up an aftercare regime. By disclosing for the first time the relevant risk to stakeholders, the candidate agrees to the conditions and the employer accepts or rejects the after-care proposal.

Q. What if we get a red light result or an orange light result as part of existing workforce screen?

The solution reveals hidden risks and highlights weak areas in an anonymised and aggregated way. Our consultants offer risk mitigation advice, tools and even board level presentations to discuss implementation recommendations. Example actions might be adjusting HR policies & practice, remedial training in certain areas, setting up an employee assistance program, or ongoing social media monitoring etc. as part of PSPF13 ongoing suitability.

A visual representation of a company's insider threat vulnerability landscape.



🟢	Favourable ("Green") for low or very low-risk profiles where no issues have been identified, or there is a high level of confidence that the residual risk is acceptable.
🟠	Caution ("Amber") for moderate-risk profiles where there is a certain amount of residual risk which means there are doubts that the mitigating factors have fully outweighed the aggravating factors.
🔴	Adverse ("Red") for high-risk profiles where the mitigating factors have not convincingly outweighed the aggravating factors. If the person was applying for a national security clearance, there is a good chance they would be denied.

By using Cleard Life Vetting Agency's unique suitability clearance & personnel security risk assessment tool, the background check will scan twenty-one areas of a person's life for potential security vulnerabilities.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

Q. What information should be furnished by the infrastructure entity to assist the suitability screening process?

- NIST 800-53 (Rev 4). “Organisations should correlate both technical and nontechnical information. Human resource records are especially important, as there is compelling evidence to show that insider crimes are often preceded by non-technical behaviours in the workplace.”
- Results/summary from HR checks: eg. Adverse Ref reports (eg. allegations in the workplace), probable CV discrepancies, potentially adverse external checks, disclosable court outcomes, unfavourable social media posts etc.
- Stop unnecessary duplication! Don’t send original checks – id, ref reports etc.

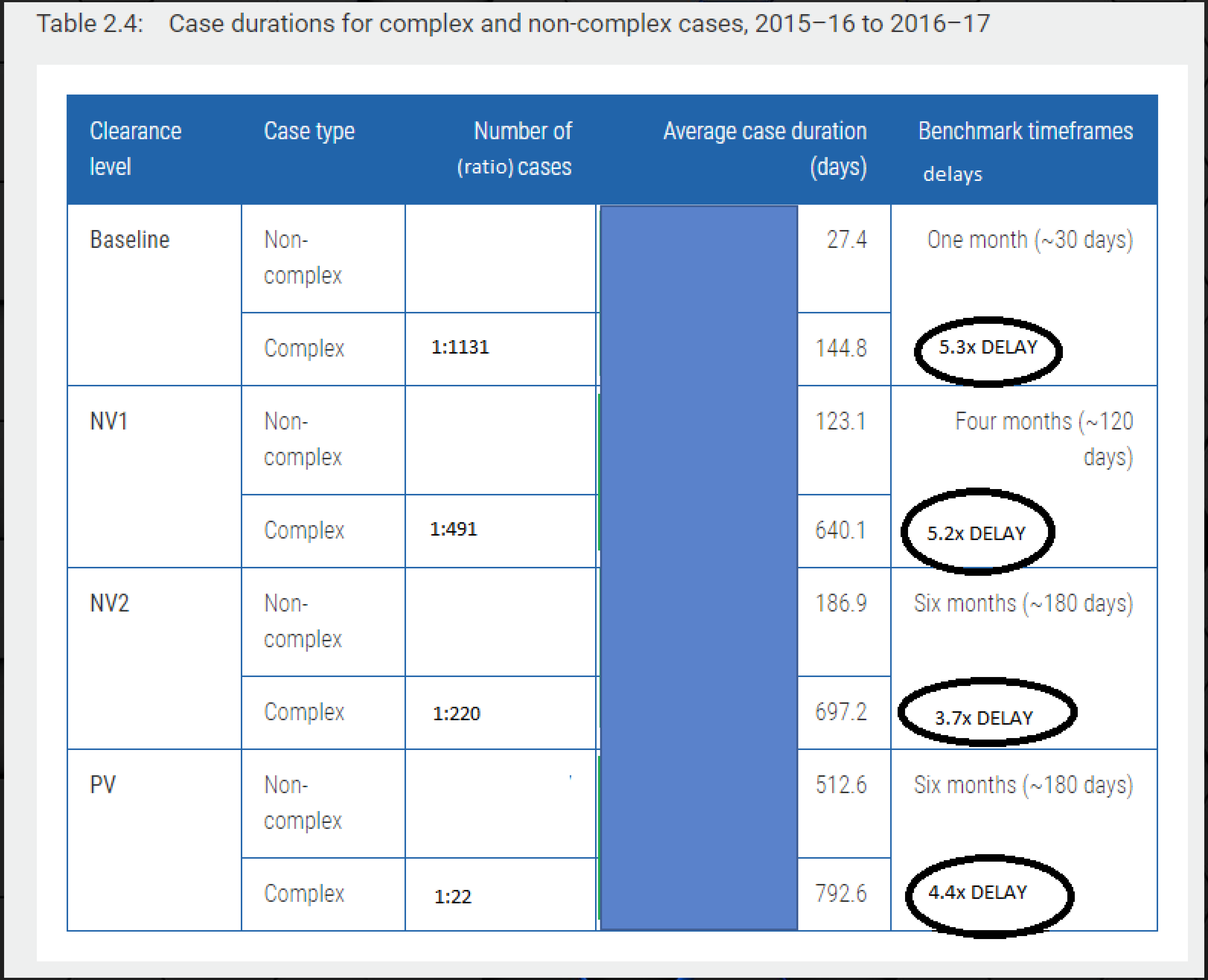


Table 2.4: Case durations for complex and non-complex cases, 2015–16 to 2016–17

Clearance level	Case type	Number of (ratio) cases		Average case duration (days)	Benchmark timeframes delays
Baseline	Non-complex		[redacted]	27.4	One month (~30 days)
	Complex	1:1131	[redacted]	144.8	5.3x DELAY
NV1	Non-complex		[redacted]	123.1	Four months (~120 days)
	Complex	1:491	[redacted]	640.1	5.2x DELAY
NV2	Non-complex		[redacted]	186.9	Six months (~180 days)
	Complex	1:220	[redacted]	697.2	3.7x DELAY
PV	Non-complex		[redacted]	512.6	Six months (~180 days)
	Complex	1:22	[redacted]	792.6	4.4x DELAY

Source: ANAO Audit of AGSVA

How fast & and how many?

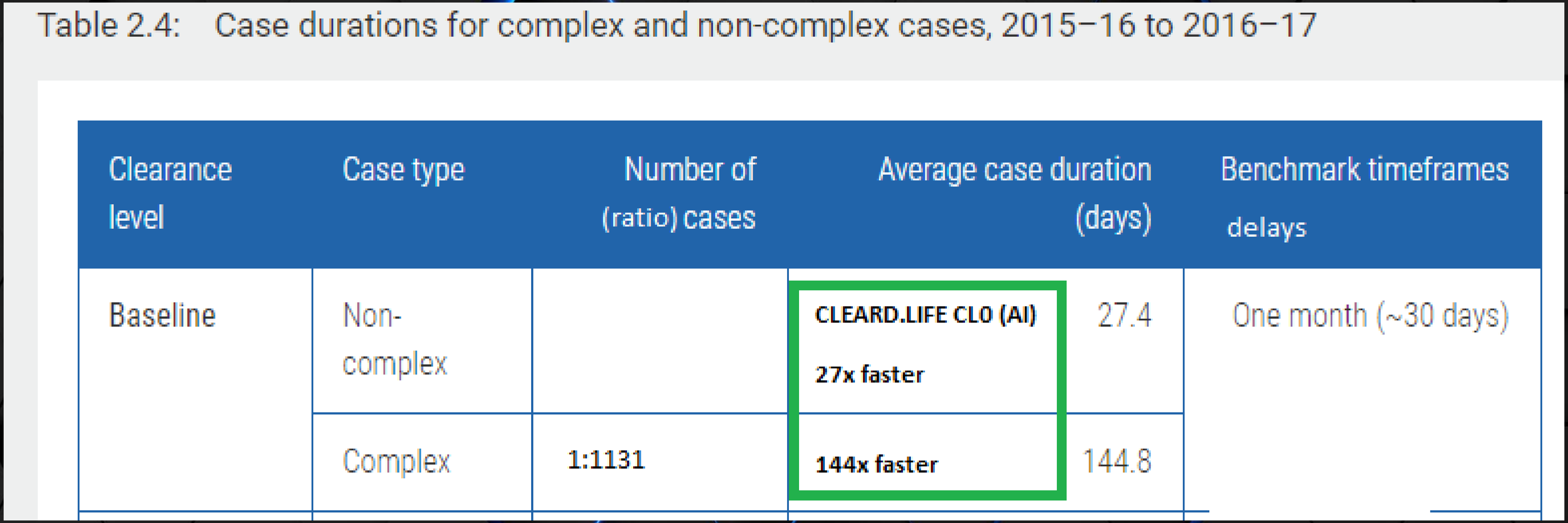
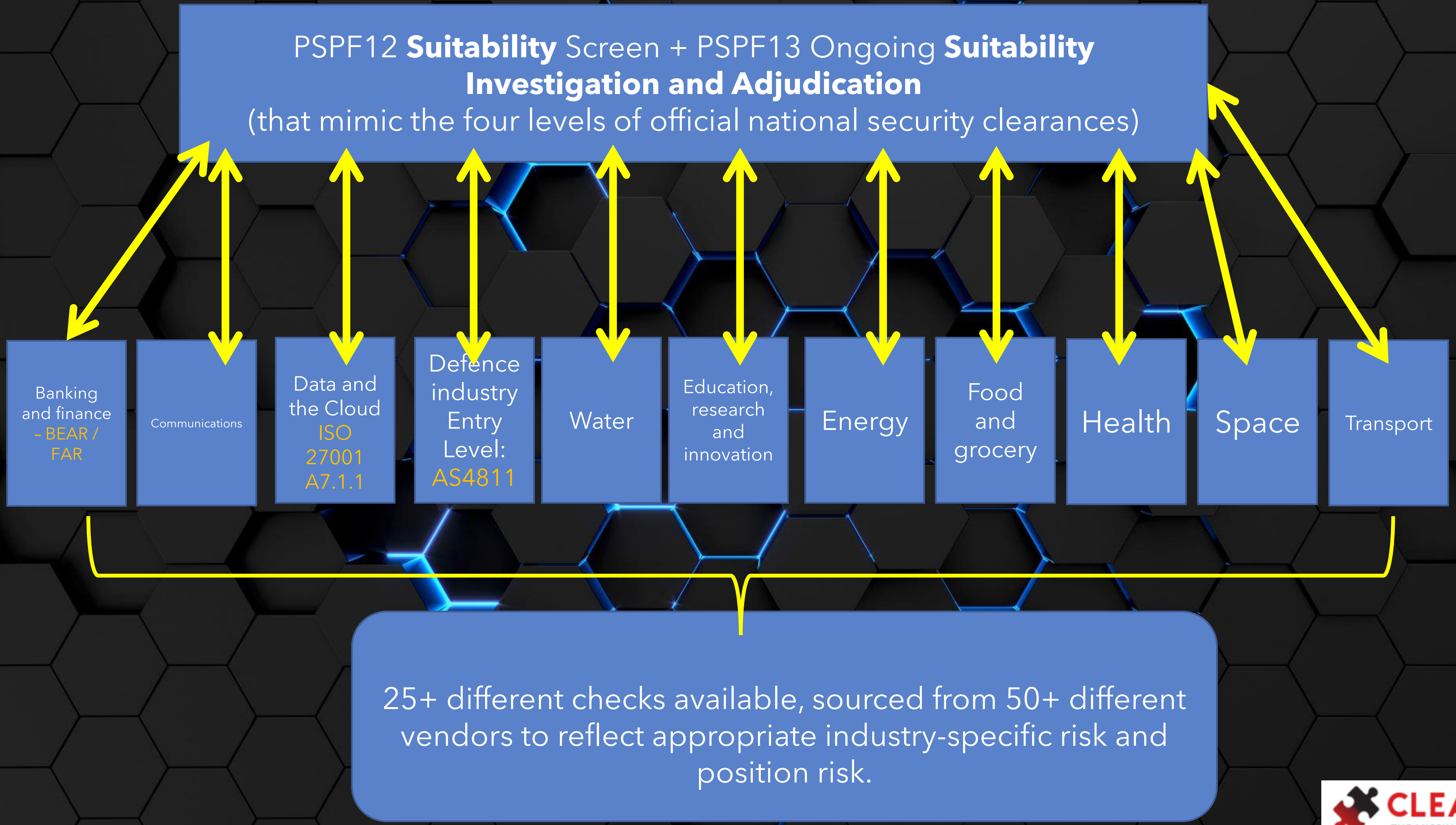


Table 2.4: Case durations for complex and non-complex cases, 2015–16 to 2016–17

Clearance level	Case type	Number of (ratio) cases	Average case duration (days)	Benchmark timeframes delays
Baseline	Non-complex		CLEARD.LIFE CLO (AI) 27x faster 27.4	One month (~30 days)
	Complex	1:1131	144x faster 144.8	

Scalability: ability to process more than 250,000 assessments per year vs 10,000 Baselines, using similar number of FTE vetting officers (15).

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE



PSPF12 **Suitability** Screen + PSPF13 Ongoing **Suitability Investigation and Adjudication**
(that mimic the four levels of official national security clearances)

- Banking and finance – BEAR / FAR
- Communications
- Data and the Cloud ISO 27001 A7.1.1
- Defence industry Entry Level: AS4811
- Water
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport

25+ different checks available, sourced from 50+ different vendors to reflect appropriate industry-specific risk and position risk.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

Dissecting the Employer Disconnect

“40% of the workforce changes jobs annually and the result is a billion dollar market just for products related to recruitment, background checks, advertisement, assessment and interviewing.”

source: hrexecutive.com

Q. Would a ‘transferable’ civilian suitability clearance or a “Seek/Indeed” “trust badge” or private or public verifiable character credential system assist in reducing duplication and waste?

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

Any questions?

Cleard Life Vetting Agency (CLVA) and Crown Vetting: Commonwealth vetting panel member and strengthening the national integrity system since 2010.

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE