****

OFFICIAL: Sensitive (from first entry)

**Justice and Community Safety Directorate**

**Security and Emergency Management**

# Security Clearance Eligibility Tool and Risk Assessment

The purpose of this Eligibility Assessment Tool is to allow entities to assess a position or group of postions that have been identified as high risk (under the ACT Protective Security Framework), to determine if the holders of these positions need to hold a security clearance to mitigate the protective security risks associated with the position.

Users should use the table on pages 3 and 4 below to identify the types and scale of risks, whether there are mitigations, and determine whether a security clearance is justified as a means to mitigate the risks identified.

The intent of the tool is to assess the overall risks or impacts of the position, considering other management measures in place, and determining whether a security clearance is needed, and what level that should be.

## Purpose of having security vetted personnel

As outlined on the [Australian Government Security Vetting Agency (AGSVA) website](https://www.defence.gov.au/security/clearances/about/overview#purpose), the purpose of the security vetting process is to determine whether an individual is suitable to hold a security clearance–that is, whether they possess and demonstrate an appropriate level of integrity.

Some positions in the ACT Government involve the handling of sensitive information or management of high value assets and require additional checks to ensure the person is of sound character, demonstrates reliability and is not vulnerable to improper influence.

It is important that a security clearance level accurately reflects the requirements of the position and the ‘need-to-know’. A higher security clearance level than is required creates a risk of staff accessing systems or information they shouldn’t.

## Determining the required security clearance level

The manager assessing the position should use the factors as identified in the *Position Assessment Tool* and *Business Impact Level Assessment Tool to* determine what security clearance level is required, or if one is not required at all.

The security clearance level for a position is determined by the type of information, assets and/or systems that the position will access as part of their role. Additionally, consideration should be given to whether there are other mitigations in place that reduce the risk of misuse of access. The table below sets out at a high level the clearance level that might be needed for a position.

|  |  |  |
| --- | --- | --- |
| **Clearance level** | **Level of security classified resources** | **Activities in the role** |
| Baseline | Classified resources up to and including PROTECTED. | Access to large numbers of tender documents or business cases, large quantities of aggregated information.Responsibility for large sums of money or high value items. Handling large amounts of sensitive information. |
| Negative Vetting Level 1 | Classified resources up to and including SECRET.Temporary access to TOP SECRET in certain circumstances. | Require access to security classified information or systems. Members of specific security-related committees.Cabinet Office staff, CMTEDD IGR staff, JACS SEMD staff.Directors-General or Deputy Directors-General. |
| Negative Vetting Level 2 | Classified resources up to and including TOP SECRET. | Director-General or Deputy Director-General who also have specific security-related responsibilities (Director-Generals seeking this clearance must have Head of Service endorsement).  |

Additionally, the frequency of access and likelihood of risk must be considered. If a position occupant will access information or systems infrequently, the risk is lower than a position occupant who will access the information or systems daily. Similarly, the likelihood of risk will differ between positions as some information or assets may have little business level impact should they be compromised.

The *Position Assessment Tool* allows managers to identify the type of access a position will have to resources, potential mitigations and subsequently allow an assessment of the overall risk of the position.

The *Business Impact Level Assessment Tool* can be used to determine the consequences that might come from the compromise of information or resources by a position’s occupant. The *BIL Tool* assists users to quantify the scale of impact of breaches of information in various areas so the outcome can be reflected in the *Position Assessment Tool*. The [ACTIA Risk Matrix](https://actss.service-now.com/sharedservices?id=knwl_article&sys_id=5c3b20d1dbed80544ee430ee7c9619ff) is another tool that can be used to assess the impact of compromise of ACT Government resources for the purposes of determining the business impact level.

Managers should complete the form and on the basis of the responses, including a description of the risk of the position, the mitigations in place and make a determination on of balance of whether the position needs a clearance, and if so, what clearance is needed.

## FAQs

*If a position is identified as a Position of Trust or Designated Security Assessed Position but is only a temporary or short-term contract, should a security clearance be requested?*

The security vetting process can take from a few weeks to a few months to complete depending on the [security clearance level](https://www.defence.gov.au/security/clearances/about/vetting-time-frames) and the background of the individual.

If the individual is on a temporary or short-term contract (between 3-6 months), consideration should be given to whether measures can be put in place to ensure they are able to do the work of the position, while not having access to sensitive systems or information.

*If an individual already has a security clearance higher than what is required for the position, can the position’s security clearance level be increased?*

No, the position’s security clearance level will not be increased as a result of the successful applicant having a higher security clearance level. The security clearance level is a consideration of the requirements of the position, and not the individual who occupies it.

While a security clearance may not be sponsored at the higher level due to it not being required, the individual may be able to ‘reactivate’ the higher level (if it is before their revalidation) should they move into a new position and the sponsoring directorate/department accepts responsibility of their security clearance level. More information is in the *Security Clearance Policy*.

|  |
| --- |
| **Position details** |
| Position title(Position Description should be attached) |  |
| Position number/s |  |
| Classification |  |
| Division/Branch |  |
| Directorate |  |
| Reason for assessment | [ ]  New position/s | [ ]  Change in position/s  |
| Type of employment | [ ]  Permanent | [ ]  Temporary  |
| Current security clearance level required | [ ]  None | [ ]  Baseline | [ ]  NV1 | [ ]  NV2 |
| Security clearance level sought | [ ]  None | [ ]  Baseline | [ ]  NV1 | [ ]  NV2 |
| Is a security clearance required for a committee this position will be a member of? | [ ]  Yes. Committee: |
| **Risk assessment** |
| What information/resources/systems will the positions use or have access to? | [ ]  Personal information[ ]  Security or intelligence information[ ]  Cabinet information[ ]  Commonwealth information or data holdings[ ]  Health records[ ]  Financial systems[ ]  ICT system or network administrator[ ]  CCTV system access or surveillance[ ]  Committees[ ]  High value assets[ ]  Other:  |
| What is the highest level of information or systems the position will be required to access? | [ ]  Official: Sensitive | [ ]  CABINET | [ ]  PROTECTED | [ ]  SECRET | [ ]  TOP SECRET |
| What is the Business Impact Level of information or system compromise? | [ ]  Low | [ ]  Medium | [ ]  High |
| Regularity of access to information or systems? | [ ]  Frequent  | [ ]  Regular | [ ]  Rarely |
| What sort of access to systems will the position have? | [ ]  Privileged | [ ]  Administrator | [ ]  Aggregated information | [ ]  ASN |
| What will those systems be? |  |
| Regularity of access to systems? | [ ]  Routine | [ ]  Specific circumstances |
| Will the position have access to financial systems/delegations? | [ ]  Yes | [ ]  No |
| Will the position manage high value assets? | [ ]  Yes | [ ]  No |
| Level of financial delegation | [ ]  Low ($50,000)[ ]  Medium ($500,000)[ ]  High ($5,000,000) |
| Overall assessment of the risk of misuse in this position. |  |
| What mitigations are in place (or could reasonably be implemented) to prevent misuse of this access to resources? |  |
| Summary justification for clearance |  |
| **Position assessor** |
| Name of manager |  |
| Position |  |
| Date and signature |  |
| **Security clearance determination - Agency Security Advisor to complete** |
| What are the identified business impact levels relating to the position? | [ ]  Low | [ ]  Medium | [ ]  High |
| Comments  |  |
| Type of High-Risk Position | [ ]  Position of Trust | [ ]  Designated Security Assessed Position |
| Security clearance level supported | [ ]  None | [ ]  Baseline | [ ]  NV1 | [ ]  NV2 |
| Agency Security Advisor name |  |
| Date and signature |  |
| **High level security clearance endorsement (if required) – Director-General or Head of Service to complete**  |
| Comments  |  |
| Is the NV2 clearance supported? | [ ]  Yes | [ ]  No |
| Name of endorsing Executive |  |
| Date and signature |  |

**This form must be completed prior to the position being advertised internally or on the ACT Government Jobs website.**

**Business Impact Level Assessment Tool**

|  |  |
| --- | --- |
| **Category of impact** | **Impact level** |
| **Low business impact****(1 point)** | **Medium business impact****(2 points)** | **High business impact****(3 points)** |
|
| **Individuals (or those associated with those individuals)** | Information from routine business operations. Information about an identifiable information that is not considered sensitive | Information that would endanger the safety of a person.Information that would affect an individual’s wellbeing and/or livelihood | Information about an individual that is considered sensitive. Information that would cause discrimination, mistreatment, humiliation, or loss of dignity or safety including loss of life |
| **Entity operations, capability and service delivery**  | Information from routine business operations and services causing minor disruptions to operations or organisational assets | Information that would cause a major loss of trust in the organisation with members of the public and/or stakeholders, or breach organisational obligations resulting in an investigation  | Severe degradation in or loss of organisational capability so that the entity cannot perform functions, and a major loss of confidence in government |
| **Entity assets and finances**  | Information or system compromise would result in an insignificant impact to the entity assets or annual operating budget | Information and systems that would cause limited damage to entity assets or its annual operating budget | Substantial financial loss to an entity or loss of major entity assets |
| **Compliance with legislated obligations** | Compromise would not result in issues around legislated or regulated obligations | Information that:1. relates to issues of legal professional privilege
2. causes contract or agreement non-compliance
3. causes a failure of statutory duty
 | Information that:1. impedes the development or operation of major policies
2. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted to Cabinet
 |
| **Holdings of data and information** | A significant aggregated holding of information (or system holding the information) that, if compromised, would cause limited damage to the ACT or national interest, organisations, or individuals | A significant aggregated data holding of sensitive information (or system holding that information) that, if compromised, would cause damage to the ACT or national interest, organisations, or individuals | A significant aggregated holding of sensitive or classified information (or system holding that information) that, if compromised, would cause serious damage to the ACT or national interest, organisations, or individuals |
| **Jurisdictional relations** | Information from and systems supporting routine business operations and jurisdictional activities | Information or system compromise would cause limited damage to government and incidental damage or disruption to jurisdictional relations | Information or system compromise would damage relations with other jurisdictions |
| **Economic** | Information from or systems supporting routine business operations and services that would be unlikely to impact businesses or the economy | Compromise of information, system or asset would impact the financial viability of businesses, disadvantage organisations, or have a short-term material impact on the ACT economy | Compromise of information, system or asset would undermine the financial viability of businesses, disadvantage organisations, or have a long-term impact on the ACT economy |
| **Infrastructure** | Information that relates to routine operations and services in relation to ACT infrastructure, assets that facilitate routine operations and services | Information and systems that could lead to significant damage to ACT infrastructure, and compromise of assets that support important operations and services | Information and systems that could cause significant damage to or shutting down of significant ACT infrastructure, significant assets that support key operations and services  |
| **Crime prevention**  | Information from and systems supporting routine business operations and services | Compromise of the information, system or asset would impede the detection, investigation, prosecution of, or facilitating the commission of low-level crime | Compromise of the information, system and asset would impede the detection, investigation, prosecution of, or facilitating the commission of an offence with likely imprisonment |

*Table adapted from* [*Classification Business Impact Levels Matrix (protectivesecurity.govt.nz)*](https://protectivesecurity.govt.nz/assets/Classification/Classification_BIL-Matrix.pdf) *and* [*PSPF policy 8: Sensitive and classified information (protectivesecurity.gov.au)*](https://www.protectivesecurity.gov.au/system/files/2023-01/pspf-policy-08-sensitive-and-classified-information.pdf)*.*

Calculate overall Business impact level by assigning a value to each category of impact, according to whether the compromise of the information could have a low, medium or high impact.

|  |  |
| --- | --- |
| 1-12 | Low |
| 13-20 | Medium |
| 21-27 | High |

© Australian Capital Territory 2024

This work, the Security Clearance Eligibility Tool and Risk Assessment is licensed under a [Creative Commons Attribution 4.0 licence](http://creativecommons.org/licenses/by/4.0).
You are free to re‑use the work under that licence, on the condition that you credit the Australian Capital Territory Government as author, indicate if changes were made and comply with the other licence terms.

The licence does not apply to the ACT Government logo and images from Content Manager not licenced for reuse under creative commons.