Neil J. McRae

A Dinner Table Guide to CESG Accreditation. UKNOF 19

CESG Accreditation

- CESG is the National Technical Authority for information assurance
  - www.cesg.gov.uk
- CESG offer many Products and Services
  - GovCertUK
  - CAPS (Encryption Services)
  - CLAS (Consultancy/Partner with PS and CESG)
  - CTAS – what I'm going to talk about today is based on using this service to "reach" IL2

CTAS Accreditation

- CESG Tailored Assurance Service
  - Introduced in 2007 to improve upon CESG previous Accreditation Scheme replacing Fast Track and SYS services.
  - Tailored is the key attribute
  - Service can look at wide range of evaluations from software to network infrastructure
  - New Service called CESG Assured Service (Telecoms) should make the IL2 process slightly more straight forward for operators (I've no experience of this)

"Security Impact Levels"

- These are the most common referred to security levels.
- Accreditation is of a Information Security Management System.
- IL2 (2-2-4) – Protected (Confidentiality-Integrity-Availability)
  - IL2 covers primarily ensuring that your platform has high availability and that there are basic controls in place for access to the platform and access to the data on the platform.

CESG IL2

- Takes ISO 27K and specializes it towards Telecommunication suppliers
- Government requires IL2 for service providers to supply services.
  - Local government less so but moving in that direction
  - CESG Assured Service is now focused on this for PSN.
  - If you want to offer services to government then you are going to have to do this sooner or later.
- CESG NGN Good Practice Guide was the baseline for IL2

CESG IL2

- CESG NGN Good Practice Guide has over 100 different controls contained within it
  - a lot based upon ISO27K and has continued to evolve.
  - One control for example requires deployment of 2 factor authentication to your infrastructure.
  - Patching methodologies
  - Potentially has physical security considerations
  - May require your kit supplier and their kit to be accredited
  - But its about the Information Security Management System.
- Will require you to build RACI models.
- Much of this common sense but deployment ensures you have process, which is well understood and its audited!
- Process feels laborious, especially at the start but actually builds good practice inside your organisation.
  - Can be a challenge to manage the governance here.

CESG IL2

- With CTAS you work with a CESG approved accreditor
  - I have experience with KPMG who were very good indeed.
- Process steps:
  - Preparation of what you want you want to do.
  - Evaluate yourself with the accreditor (rinse and repeat)
  - Report - did you pass? And what do you have to fix…
  - Maintain
    - Yes this is an ongoing commitment.

CESG IL3

- This is where It gets quite serious – builds on IL2
  - Levels usually associated with specific government data security requirements
- IL3 (3-3-4) – Restricted
  - Baseline for most central government projects (In my experience) – PNN / GSI
  - Requires (SC) security cleared operatives and stronger controls on access (integrity) and stronger controls on confidentiality
  - Requires complete segregation.
  - Now typically requires encryption overlay layer, didn't before.
  - Quite expensive to build, run and operate.
    - Can't share systems – e.g. your Trouble Ticket system needs to be inside the IL3 bubble and separate to anything else
  - Can't really use offshore people in this space.

CESG IL4

- Again builds on IL3
- IL4 (4-4-4) - Confidential

- Typically requires DV (Deep Vetted) security cleared operatives.
  - Home Office / FCO / MOD

- I'd have to shoot you
- IL5 Secret and IL6 Top Secret
  - MOD / Security Services