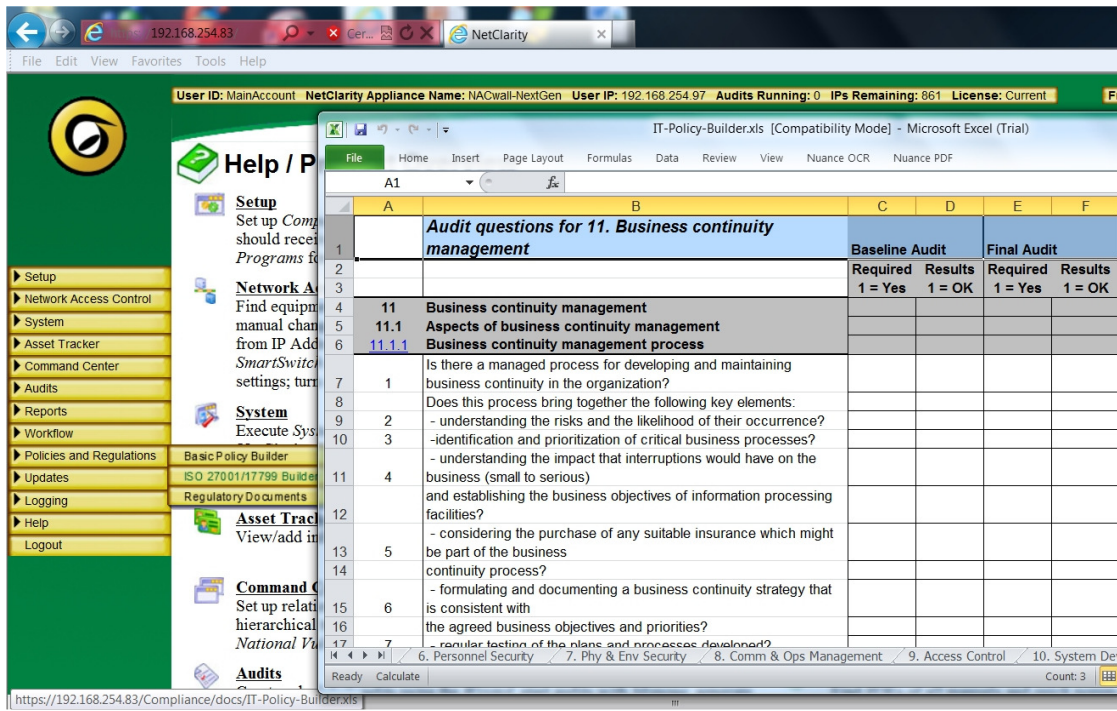


## ISO 27001 Policy Self-Assessment Tool – Why So Important?

ISO 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO). This standard formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO 27001 can therefore be formally audited and certified compliant with the standard.



		Baseline Audit		Final Audit	
		Required	Results	Required	Results
		1 = Yes	1 = OK	1 = Yes	1 = OK
11	<b>Business continuity management</b>				
11.1	<b>Aspects of business continuity management</b>				
11.1.1	<b>Business continuity management process</b>				
7	1				
8					
9	2				
10	3				
11	4				
12					
13	5				
14					
15	6				
16					
17	7				

Most organizations have a number of information security controls. Without an ISMS like the ISO 27001, however, the controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Maturity models typically refer to this stage as "ad hoc". ISO 27001 is more formal in that it requires that management to:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

NetClarity's NACwall Enterprise family of appliances are delivered with an advanced ISO27001 self-assessment auditing tool written as an excel spreadsheet with built-in hyperlinks to over 280 related word documents with sample ISO 27001 compliant policies so you can 'fill in the gaps' where you are weak and at risk of being out of compliance with this standard. By performing ISO27001 baseline and final self-assessments, delivering and implementing these policies, an organization will outdo any well recognized requirements from governments such as HIPAA/HITECH, SOX-404, GLBA, the VISA PCI-DSS and other stringent standards designed to protect consumer or customer records.