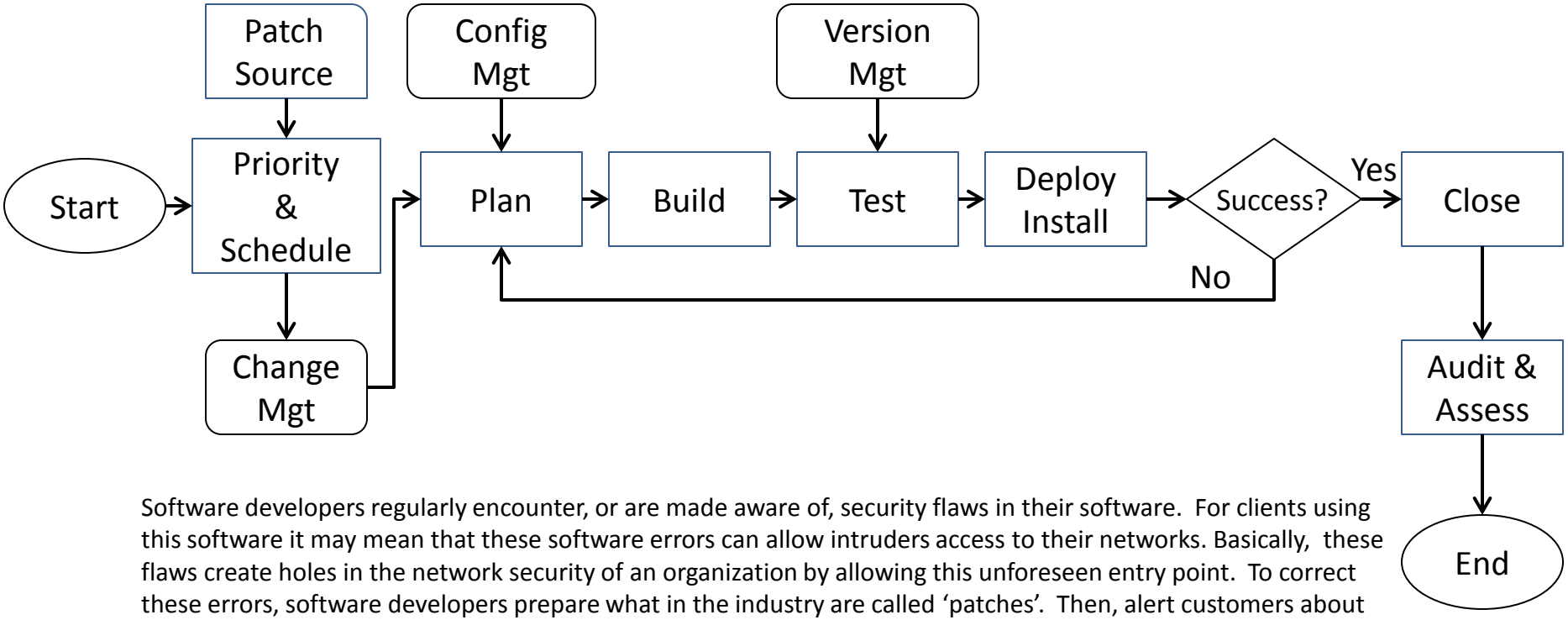
ADVANCED
CYBER SOLUTIONS, LLC.

Patch Management

The process below is an Information Technology Infrastructure Library (ITIL) IT best practice framework employed at Advanced Cyber Solutions LLC for the proper patch management.



Software developers regularly encounter, or are made aware of, security flaws in their software. For clients using this software it may mean that these software errors can allow intruders access to their networks. Basically, these flaws create holes in the network security of an organization by allowing this unforeseen entry point. To correct these errors, software developers prepare what in the industry are called 'patches'. Then, alert customers about the existence and these errors and how to correct them by installing their newly created patches. Organizations must plan to install these 'patches,' but first, they must ensure that these patches will not cause degradation of service to their networks. Degradation can mean many things, from a slowing down of service to total system crash. These may occur due to the network configuration and the interaction of multiple software platforms. To avoid network degradation, organizations need to follow a process that ensures not only the successful application of the patch, but just as importantly, the continued service of their network.