Windows中的执行体(exe文件)是在Ntoskrnl.exe上层的(内核在其下层)执行体包括以下几种函数：

* 从用户模式(Ntdll.dll)中导出的可调用函数
* 通过***DeviceIoControl***函数调用的设备驱动函数
* 从内核中导出并可以被调用而且在WDK中文档化的函数
* 从内核中导出并可以被调用但没有在WDK中文档化的函数
* 其符号已经被定义但是没有被导出的函数

执行体包含以下主要组件：

* **配置管理器**(configuration manager): 主要用于执行和管理系统记录
* **进程管理器**(process manager): 用来创建和结束进程和线程。针对进程和线程的底层能在Windows内核中实现的，执行体则在这些底层对象的基础上又加上了额外的语义和功能。
* **安全引用监视器**(security reference manager): 强制在本地计算机上实行安全策略。它守护着操作系统的资源，执行对运行时对象的保护和审计
* **I/O管理器**(I/O manager): 实现了与设备无关的I/O功能，负责将I/O请求分派到恰当的设备驱动程序以进一步处理。
* **即插即用**(PnP)**管理器**(Plug and Play manager): 为了支持某个特定的设备，确定哪些驱动程序是必需的，同时也负责加载这些驱动程序。它在设备枚举过程中，获取到每个设备的硬件资源需求。PnP管理器根据每个设备的资源需求，分配适当的硬件资源，比如I/O端口、IRQ、DMA通道和内存位置。当系统中的设备变化（增加或者移除设备）时，它还负责发送恰当的事件通知。
* **电源管理器**(power manager) 负责协调电源事件，并且产生电源管理I/O通知，发送设备驱动程序。电源管理器可以配置成：当系统空闲时，通过将CPU置于睡眠状态而降低电源消耗。单个设备的电源消耗变化可由设备驱动程序处理，但是需要电源管理器来协调
* **Windows驱动程序模型**(Window Driver Model)的**WMI例程** 允许设备驱动程序发布有关性能和配置的信息，以及接收来自用户模式WMI服务的命令。WMI信息的消费者可以运行在本地机器上，也可以在跨网络的远程机器上
* **缓存管理器**(cache manager) 提高了基于文件的I/O操作的性能，其做法是，让最近引用过的磁盘数据驻留在主内存以便快速访问（并且延迟磁盘写操作，在将更新数据发送到磁盘之前先在内存中停留一小段时间）。它利用了内存管理器对映射文件的支持来做到这一点
* **内存管理器**(memory manager) 实现了**虚拟内存**。
* **逻辑预取器**(logical prefetcher)和**Superfetch**用于加速系统和进程的启动过程。做法为，对于要在系统或进程启动过程引用的数据，它优化这些数据的加载过程。