编号：CR-MS0505

个人身份信息管理体系认证规则

（H/0）

2025-11-20 发布　　2025-11-20 实施

北京海德国际认证有限公司发布

个人身份信息保护管理体系认证规则

1 适用范围

本实施规则用于规范北京海德国际认证有限 HIC（以下简称“HIC”）开展个人身份信息保护管理体系认证活动。

2 认证依据

ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》

ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实践规范》

3 术语和定义

3.1 个人可识别信息（PII）

满足以下条件之一的信息：

1) 可用于在该信息与相关自然人之间建立关联；

2) 已直接或间接关联，或可能直接或间接关联到某一自然人。

注释：定义中的“自然人”指个人可识别信息主体。判断 PII 主体是否可识别时，需考量持有数据的隐私相关方，或其他任何一方，为在 PII 集合与自然人之间建立关联，可合理采用的所有手段。

3.2 个人可识别信息主体（PII 主体）

与 PII 相关联的自然人。

3.3 个人可识别信息控制者（PII 控制者）

决定 PII 处理目的和处理方式的隐私相关方（或多个隐私相关方），不包括为个人目的使用数据的自然人。

条目注释：PII 控制者有时会指示其他方（如 PII 处理者）代表其处理 PII，但处理责任仍由该控制者承担。

3.4 个人可识别信息处理者（PII 处理者）

代表 PII 控制者并依据其指示，处理 PII 的隐私相关方。

4 实施审核活动的人员能力要求

4.1 PIIMS 审核员，在具备 ISMS 审核员注册资格的基础上，还应具备以下通用知识：

1) ISO/IEC 27001 和 ISO/IEC 29151 相关信息安全管理和个人身份信息保护知识；

2) PIIMS 的监视、测量、分析与评价知识；

3) 与个人身份信息保护管理相关的信息安全风险知识；