

Risk Analysis

Inherent risk analysis based on proposed OmniHyper® open-source solution vs. general closed-source solutions available.

Risks	OmniHyper® Solution	General Solution
<u>TECHNOLOGY</u> protection of your investment.	<ul style="list-style-type: none"> Open-source solutions including Joomla! and WordPress, the world's largest content management systems. Client Retains IP. Not restricted to OmniHyper as provider. LOW RISK	<ul style="list-style-type: none"> Internal system with licensed/annual fees to keep updated. IP not owned by client; service provider owns code. Restricted to single provider. **HIGH RISK**
<u>CONTINUITY</u> of website operations.	<ul style="list-style-type: none"> Open-source – millions of developers globally. Ease of use with full public documentation. Multiple resources available; costs are market related. LOW RISK	<ul style="list-style-type: none"> Restricted to original developer(s) and third party companies – may be affected by staff continuity. Hard to use with limited documentation. Single resource dependency with costs dictated by provider. **HIGH**
<u>DEPENDENCY</u> on the initial service provider.	<ul style="list-style-type: none"> Open-source – Not reliant on OmniHyper®. Can be easily transferred to alternative provider. LOW RISK	<ul style="list-style-type: none"> Reliant on company's stability and longevity. Cannot be easily transferred to alternative provider. **HIGH**
<u>SEARCH</u> visibility and readability by major Search Engines (e.g. Google).	<ul style="list-style-type: none"> Google and Search Engine compliant. LOW RISK	<ul style="list-style-type: none"> (Potentially) NOT Google and Search Engine compliant with code errors giving rise to low ranking within Search Engines. **HIGH**
<u>TAXONOMY</u> of the site and data.	<ul style="list-style-type: none"> Site and content structured in accordance with international standards for data and information storage. LOW RISK	<ul style="list-style-type: none"> Limited to directory structures and definition by site developers. **HIGH**
<u>LOGICAL SECURITY</u> and access to data stored.	<ul style="list-style-type: none"> Multiple authorisation levels and 128-bit secure encryption. International security standards/compliance. LOW RISK	<ul style="list-style-type: none"> Dependant on level of inhouse expertise integration with 3rd party security components. Constant redevelopment of security modules. **MEDIUM**
<u>KEY RESOURCE</u> dependency	<ul style="list-style-type: none"> Maintenance through low level computer literacy skills. Administration of user accounts and content by non-technical persons/inhouse resource. LOW RISK	<ul style="list-style-type: none"> Maintenance through technical persons. Built by technical people for high-level web users with limited user documentation. Limited FAQ/forums. **MEDIUM**