Due diligence and Due care:

**Harris:**Due diligence is the act of gathering the necessary information so the best decision-making activities can take place.  
Due care pertains to acting responsibly and “doing the right thing.” It is a legal term that defines the standards of performance that can be expected,

**Conrad:**  
Whereas due care intends to set a minimum necessary standard of care to be employed by an organization, due diligence requires that an organization continually scrutinize their own practices to ensure that they are always meeting or exceeding the requirements for protection of assets and stakeholders. Due diligence is the management of due care, and it follows a formal process.

From the Harris definition, it looks like due diligence is gather information and due care involves actions and performance.  
From Conrad’s definition, due care is setting a standard, and due diligence involves the day to day actions.

**Due Care**  
It is also considered Legal Duty of a company. As in a company is obliged by Law to perform certain steps, if it fails to do so, then it can be held liable in court. For example, Bank should let their customers know that they will never ask for their PIN or password to avoid lawsuits or comply with laws and regulations.

**Due Diligence**  
This pertains to best practices that a company should follow to keep its head above the water(keep itself secure). If a company fails to implement these measures, it might face an attack but might not be legally liable. For example, performing penetration tests or employee background checks to find holes would be due diligence as it might not be mandated by law but its a good practice.

Due diligence  
– Research what threats exists for websites running IIS (and stay up-to-date through newsletters, mailing lists, etc)  
– Research what threats affect various applications part of the website (such as ASP.NET or PHP frameworks, databases, SSL certificates, mail servers, authentication, etc)  
– Determine what are the common protection mechanisms (encryption, firewalls, A/V, backup, etc)  
– Design IT security policies related to IIS-based websites

Due care  
– Implement IT security policies  
– Constantly monitor website as per security policies  
– Keep the website updated with latest patches, hotfixes (according to change control policy)  
– If the site is compromised, identify and correct the problem, change passwords, notify users, etc (again, as per IT Security policy set in “Due diligence”)

So in the end, due diligence is creating a good security policy while due care is making sure that the security policy is implemented and followed to the letter.

Due care is much wider in scope then due diligence and due care encompass due diligence in itself as one of the key areas.

Authorization and Authentication:

* **Authentication** is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating.
* **Authorization** is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is authorization.
* Authentication is about who somebody is.
* Authorisation is about what they're allowed to do.